7 BOOKS IN 1

BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES

BITCOIN MINING

BLOCKCHAIN BASICS

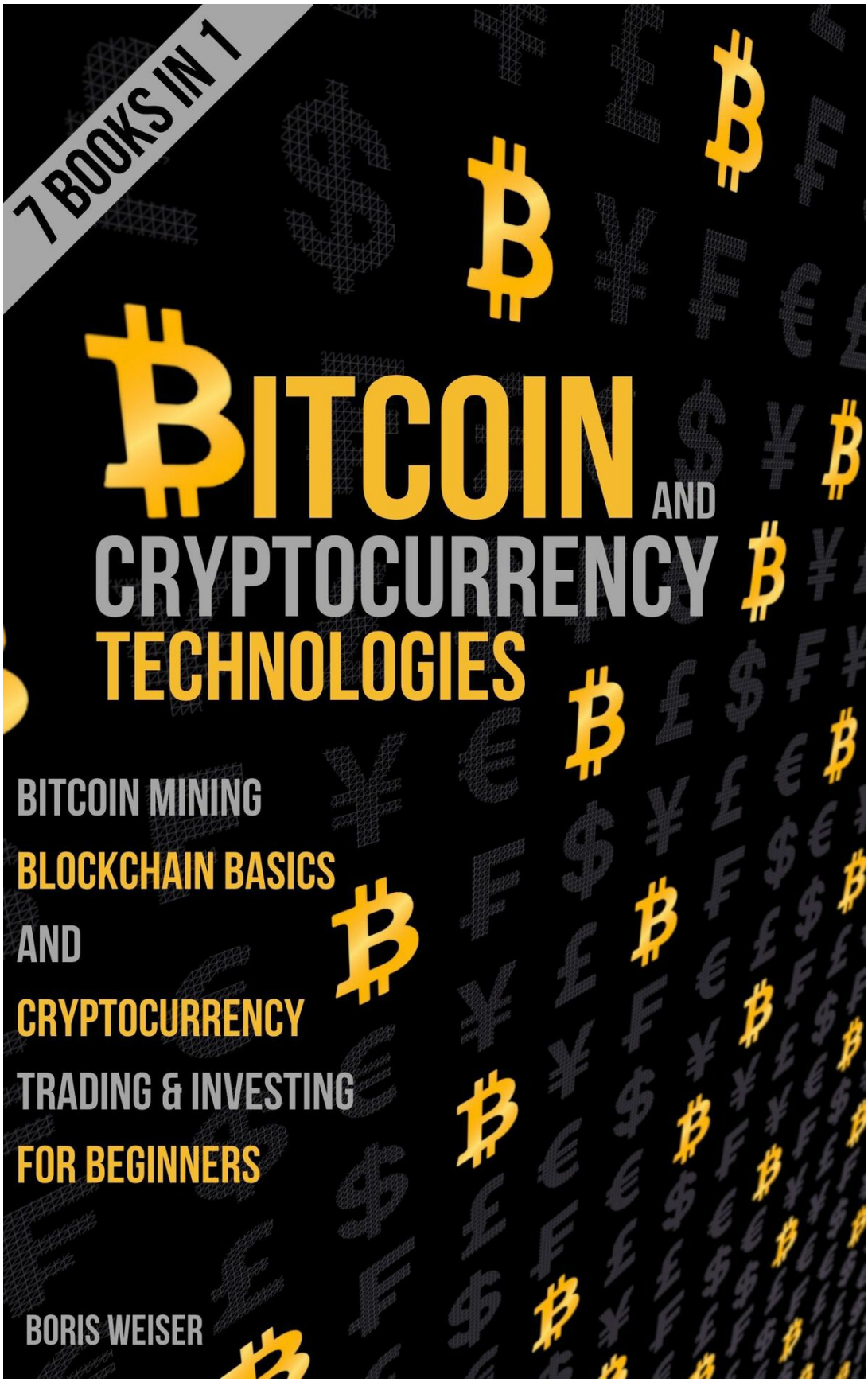
AND

CRYPTOCURRENCY

TRADING & INVESTING

FOR BEGINNERS

BORIS WEISER


7 BOOKS IN 1
BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES
BITCOIN MINING
BLOCKCHAIN BASICS
AND
CRYPTOCURRENCY
TRADING & INVESTING
FOR BEGINNERS
BORIS WEISER

BITCOIN AND CRYPTOCURRECNY TECHNOLOGIES

BITCOIN MINING, BLOCKCHAIN BASICS
AND
CRYPTOCURRENCY TRADING & INVESTING FOR BEGINNERS

7 BOOKS IN 1

BOOK 1
BITCOIN IS BLOCKCHAIN AND HERE IS WHY!

BOOK 2
LEARN FAST WHY BITCOIN IS THE INVENTION OF THE 21ST CENTURY

BOOK 3
THE ADVENTURES OF THE CYPHERPUNK BILLIONAIRE CRYPTOREBEL

BOOK 4
CRYPTOCURRENCY INVESTING USING HOT & COLD WALLETS

BOOK 5
17 PRIVACY BASED COINS YOU SHOULD KNOW ABOUT

BOOK 6
MUST HAVE TOOLS, BEST EXCHANGES AND TRADING STRATEGIES

BOOK 7
TRADING BOTS, CANDLESTICK PATTERNS AND TRADING PSYCHOLOGY

BORIS WEISER

COPYRIGHT

ALL RIGHTS RESERVED. NO PART OF THIS BOOK MAY BE REPRODUCED IN ANY FORM OR BY ANY ELECTRONIC, PRINT OR MECHANICAL MEANS, INCLUDING INFORMATION STORAGE AND RETRIEVAL SYSTEMS, WITHOUT PERMISSION IN WRITING FROM THE PUBLISHER.

COPYRIGHT © 2021 BORIS WEISER

Disclaimer

This book is produced with the goal of providing information that is as accurate and reliable as possible. Regardless, purchasing this book can be seen as consent to the fact that both the publisher and the author of this book are in no way experts on the topics discussed within and that any recommendations or suggestions that are made herein are for entertainment purposes only. Professionals should be consulted as needed before undertaking any of the action endorsed herein. Under no circumstances will

any legal responsibility or blame be held against the publisher for any reparation, damages, or monetary loss due to the information herein, either directly or indirectly. This declaration is deemed fair and valid by both the American Bar Association and the Committee of Publishers Association and is legally binding throughout the United States. The information in the following pages is broadly considered to be a truthful and accurate account of facts and as such any inattention, use or misuse of the information in question by the reader will render any resulting actions solely under their purview. There are no scenarios in which the publisher or the original author of this work can be in any fashion deemed liable for any hardship or damages that may befall the reader or anyone else after undertaking information described herein. Additionally, the information in the following pages is intended only for informational purposes and should thus be thought of as universal. As befitting its nature, it is presented without assurance regarding its prolonged validity or interim quality. Trademarks that are mentioned are done without written consent and can in no way be considered an endorsement from the trademark holder.

Table of Contents – Book 1

Should you read this book?

Introduction

Chapter 1 How Blockchain is connected to Bitcoin

Chapter 2 A brief history of finance

Chapter 3 Bitcoin fundamentals

Chapter 4 The Publication of Whitepaper

Chapter 5 The Author of the Bitcoin Whitepaper

Chapter 6 The Distributed Ledger System

Chapter 7 Who are the Bitcoin Miners

Chapter 8 How Bitcoins are created

Chapter 9 How secured is the Blockchain

Chapter 10 Comprehending Business purposes

Chapter 11 Introduction to Blockchain Attributes

Chapter 12 Peer-to-peer network

Chapter 13 Understanding Hashing

Chapter 14 Cryptography Basics

Chapter 15 What is a Digital Signature

Chapter 16 Comprehending Logarithms

Chapter 17 Understanding Diffie-Hellman Key Exchange

Chapter 18 Elliptic Curve Cryptography

Chapter 19 How to Encode arbitrary data

Chapter 20 What is a Checksum

Chapter 21 Understanding Vanity Addresses

Chapter 22 Understanding the Double Spending problem

Chapter 23 What is the Great Ledger

Chapter 24 Comprehending the chain of Blocks

Chapter 25 Understanding Testnet and Faucets

Chapter 26 Segregated Witness

Chapter 27 Transaction malleability

Chapter 28 What is a Soft and Hard fork

Chapter 29 What is Lightning Network

Table of Contents – Book 2

Chapter 1 The importance of cryptocurrency

Chapter 2 Defining Money aka Medium of Exchange

Chapter 3 Trusted third parties & Quantitative easing
Chapter 4 Double Spending Problem & Solution
Chapter 5 The revolution of Crypto & Digital Cash
Chapter 6 Centralization and decentralization.
Chapter 7 The rise of the Cypherpunks
Chapter 8 The MAN of the 21st Century!
Chapter 9 The Distributed Ledger System
Chapter 10 Transaction validation
Chapter 11 Bitcoin mining fundamentals
Chapter 12 Block reward process
Chapter 13 Block Validation process
Chapter 14 Transaction Fees
Chapter 15 Supply and demand
Chapter 16 Network Effects & BTM-s
Chapter 17 Market Manipulation & Price Predictions
Chapter 18 The best time to buy bitcoins!
Chapter 19 The worse time to buy bitcoins!
Chapter 20 Button line on buying bitcoins
Chapter 21 Why would you use Bitcoin?
Chapter 22 Bitcoin is dead
Chapter 23 Bitcoin is a scam
Chapter 24 Bitcoin is a bubble
Chapter 25 Bitcoin is a stock
Chapter 26 Bitcoin is a pyramid scheme
Chapter 27 Bitcoin Skills Described

Table of Contents – Book 3

Chapter 1 Early timeline from Public Evidences
Chapter 2 Writing style of Satoshi
Chapter 3 Satoshi’s Cryptography Skillsets
Chapter 4 Satoshi’s Written Communication Skills
Chapter 5 Satoshi’s DOB
Chapter 6 Publishing the Bitcoin Software
Chapter 7 Satoshi’s identity
Chapter 8 Satoshi is an Individual
Chapter 9 Satoshi Candidates No1
Chapter 10 Satoshi Candidates No2

Chapter 11 Satoshi Candidates No3
Chapter 12 Satoshi Candidates No4
Chapter 13 Satoshi Candidates No5
Chapter 14 Satoshi Candidates No6
Chapter 15 Other Rumours, Assumptions and Theories
Chapter 16 How Can Satoshi Prove himself
Chapter 17 How did Satoshi left the project?
Chapter 18 Why did Satoshi vanish?
Chapter 19 Does it matter who Satoshi is?
Chapter 20 Will we ever meet Satoshi?
Chapter 21 Additional resources and references

Table of Contents – Book 4

Chapter 1 What is a Cryptocurrency Wallet
Chapter 2 How Cryptocurrency Wallet works
Chapter 3 The Importance of Cryptocurrency Wallet
Chapter 4 Online Wallets aka Hot Wallets
Chapter 5 Paper Wallets
Chapter 6 Desktop Wallets
Chapter 7 Mobile Wallets
Chapter 8 Cold Wallets
Chapter 9 Tips to choose the right Wallet
Chapter 10 Blockchain Wallet Online Installation
Chapter 11 Blockchain Wallet Mobile Installation
Chapter 12 Coinbase Wallet Online Installation
Chapter 13 Coinbase Mobile wallet Installation
Chapter 14 JAXX Liberty desktop Wallet Installation
Chapter 15 JAXX mobile Wallet Installation
Chapter 16 Exodus Wallet
Chapter 17 TREZOR
Chapter 18 Trezor One Versus Trezor Model T
Chapter 19 How to setup the Trezor Model T
Chapter 20 How to setup KeepKey
Chapter 21 Ledger Nano
Chapter 22 How to setup Ledger Nano S
Chapter 23 How to setup the Ledger Nano X
Chapter 24 How to upgrade the Ledger Nano Firmware

Chapter 25 Additional Hardware wallets
Chapter 26 How many wallets should you have
Chapter 27 Wallet diversification: Scenario 1
Chapter 28 Wallet diversification: Scenario 2
Chapter 29 How to Buy and Transfer bitcoins on Hot and Cold Wallets
Chapter 30 Why you must own your private keys
Chapter 31 Hot Wallet Hacks
Chapter 32 How to avoid Hardware wallet scams
Chapter 33 Best Practices to Guard against MITM attacks

Table of Contents – Book 5

Chapter 1 Defining Anonymity
Chapter 2 Why Privacy coins needed
Chapter 3 Cryptocurreny Basics
Chapter 4 How Privacy Coins Work
Chapter 5 ICO Insanity
Chapter 6 How to avoid being scammed
Chapter 7 Pump and dump
Chapter 8 Komodo
Chapter 9 DeepOnion
Chapter 10 Solaris
Chapter 11 Sumokoin
Chapter 12 Firo aka Zcoin
Chapter 13 AEON
Chapter 14 Bytecoin
Chapter 15 Navcoin
Chapter 16 PIVX
Chapter 17 DASH
Chapter 18 Zcash
Chapter 19 Monero
Chapter 20 Verge
Chapter 21 Beam
Chapter 22 Grin
Chapter 23 Particl
Chapter 24 Horizon / ZenCash
Chapter 25 Overview of Privacy Coins
Chapter 26 Privacy Coins No1 Privacy Based Coin

Chapter 27 Cryptocurrency regulations
Chapter 28 SEC
Chapter 29 CFTC
Chapter 30 FinCen

Table of Contents – Book 6

Chapter 1 Portfolio Tools: Blockfolio
Chapter 2 Portfolio Tools: Messari
Chapter 3 Portfolio Tools: Altpocket
Chapter 4 Portfolio Tools: Delta
Chapter 5 Portfolio Tools: Cointracking
Chapter 6 Market Manipulation: Pump and Dump
Chapter 7 Market Manipulation: Order book spoofing
Chapter 8 Market Manipulation: Wash trading
Chapter 9 Market Manipulation: Stop loss hunting
Chapter 10 Market Manipulation: FUD
Chapter 11 Bitcoin Options: Option Theory
Chapter 12 Bitcoin Options: Option Strategies
Chapter 13 How to build options strategies on Deribit
Chapter 14 Extensive potential for Option markets
Chapter 15 Crypto Trader TAX tool
Chapter 16 Bear.Tax tool
Chapter 17 CoinTracking as a TAX Tool
Chapter 18 Koinly TAX Tool
Chapter 19 No trading formula
Chapter 20 Taking a loss – now what!
Chapter 21 Why you must place Stop losses
Chapter 22 Trading markets and Overtrading
Chapter 23 Analysis Paralysis
Chapter 24 Leverage
Chapter 25 Bad Broker Advice
Chapter 26 Choosing the wrong Exchange
Chapter 27 Overconfidence
Chapter 28 Market Activity & Initial Research
Chapter 29 Researching Technical Elements
Chapter 30 Double-check the Source
Chapter 31 Checking Upgrades and Roadmap

Chapter 32 Understanding Crypto Market Cycles
Chapter 33 Dynamics between Bitcoin and altcoins
Chapter 34 Comprehending Tokenomics
Chapter 35 Technical Indicators
Chapter 36 Exit Strategy
Chapter 37 Crypto Exchanges: Coinbase Pro
Chapter 38 Crypto Exchanges: Uniswap
Chapter 39 Crypto Exchanges: Binance
Chapter 40 Crypto Exchanges: FTX
Chapter 41 Leveraged Trading Basics
Chapter 42 BitMEX & BTC Futures
Chapter 43 Leverage Trading Strategies
Chapter 44 How Exchanges make money
Chapter 45 How to use leverage responsibly

Table of Contents – Book 7

Chapter 1 dYdX: Margin Trading Features
Chapter 2 dYdX: Lending & Borrowing
Chapter 3 dYdX: Margin Trading Step-by-step
Chapter 4 dYdX: Spot Trading & Lending Step-by-step
Chapter 5 dYdX: Trading BOTs
Chapter 6 Introduction to Trading Bots
Chapter 7 Trading Bots: TradeSanta
Chapter 8 Trading Bots: Shrimpy
Chapter 9 Trading Bots: Gunbot
Chapter 10 Trading Bots: Crypto Hopper
Chapter 11 Trading Bots: 3commas
Chapter 12 Key metrics signals & Red flags
Chapter 13 Volume & Liquidity
Chapter 14 Project & Dev Activity
Chapter 15 Comprehending the Project
Chapter 16 Artificial Perception of Demand
Chapter 17 Crypto.com: Interest earning tool
Chapter 18 Crypto.com: VISA Card with Cash back
Chapter 19 Crypto.com: Trading tool
Chapter 20 100x Altcoin Research: Screening Process
Chapter 21 100x Altcoin Research: Trading Volume & Exchange activity

Chapter 22 100x Altcoin Research: Onchain Metrics
Chapter 23 100x Altcoin Research: Development Activity
Chapter 24 100x Altcoin Research: Project Uniqueness
Chapter 25 100x Altcoin Research: Adoption & Community Support
Chapter 26 Trading Tips: Option Moneyness
Chapter 27 Trading Tips: Put Call Ratio
Chapter 28 Trading Tips: Options Skew
Chapter 29 Trading Tips: Market Parameters
Chapter 30 Trading Tips: Options Expiry Dates
Chapter 31 Bullish Candlestick Patterns
Chapter 32 Bearish Candlestick Patterns
Chapter 33 Continuation Candlestick Patterns
Chapter 34 Trading Tips for Success
Chapter 35 What is Implied Volatility
Chapter 36 Why Implied Volatility is Important
Chapter 37 What is Implied Volatility Rank
Chapter 38 Trading Psychology: Gambler's Fallacy
Chapter 39 Trading Psychology: Confirmation Bias
Chapter 40 Trading Psychology: The law of Small Numbers
Chapter 41 Trading Psychology: The Survivorship Bias
Chapter 42 Trading Psychology: Correlation
Chapter 43 Trading Psychology: Hindsight Bias
Chapter 44 Trading Psychology: Recency & Attribution Bias
Chapter 45 Trading Psychology: Sung Cost Fallacy
Chapter 46 Trading Psychology: Winners & Losers
Chapter 47 Step by step checklist for a Trading Plan
Chapter 48 How to set up a Trade Order
Conclusion

Should you read this book?

While some people think that Bitcoin is the main focus, Blockchain is Bitcoin's legacy. Blockchain is the technology behind Bitcoin, the revolutionary “virtual currency” that is changing the way people do business. Technology giants such as Intel, Microsoft, Cisco Systems, and Dell already invested in learning about Blockchain. The world’s largest Banks and Financial Institutions already created their own Cryptocurrency, using Blockchain technology. Fin-Tech Companies realized that Smart contracts are changing the way of doing Business, using the Blockchain platform. There are thousands of new start-ups investing every day into Blockchain, adapting to the technology of the future! A single Banking system can save between 8-15 Billion dollars per year, using Blockchain. Blockchain technology is already terminating trusted third-party services, replacing them with mathematical algorithms and digital signatures. Faster and cheaper payment transactions, in fact, employee payments can be made not daily, but every second. Better Data security by eliminating single point of failure. 100% Availability, using a fully decentralized peer-to-peer network, data will always be available. Blockchain will revolutionize a wide variety of businesses. Blockchain technology is influencing the future of doing Business, therefore, instead of falling behind, take advantage now, and learn how to master Blockchain today! Communication already in motion and visible between Person to Person, Business to Business and Machine to Machine. This book has lots of in depth information that will help you to comprehend Blockchain technology. It is a detailed guide on all Blockchain attributes and how the technology works behind Bitcoin. This guide is an excellent choice to gain a better understanding of what Blockchain is, how it improves data integrity, how it fundamentally changes the future of doing business and how it enhances data security. There are plenty of books on this subject in the market, thanks again for choosing this one! Every effort was made to ensure the book is riddled with as much useful information as possible. Please enjoy!

Introduction

This book includes 4 manuscripts.

Book 1

Book 1 will avoid technical details to provide a better understanding to those who are new to this technology. There are certain terms that some technical background in Information Technology would help understand. However, it's not essential. Everyday English has been used through this book to avoid confusion, and this book will take you by the hand and show you step-by-step how digital currency was born. For better understanding, we go back in time, and summarize the history of finance, then explain what has triggered the birth of several cryptocurrencies in our current society. Next, we analyse the theory and the primary focus behind the inventor of Bitcoin. Then take a closer look at the possible candidates of the birth father of Blockchain in more depth. Next, we briefly analyse what the distributed ledger system is, and how it is operated. Followed by the introduction of the miners, who they are, and what is their responsibility. Then it moves on to the process of how each block gets created, then how they eventually create a chain, which we call Blockchain. We will also go into more detail of what security measurements we have in place on the Blockchain. Next, we will focus on the understanding of the reason why this technology will change the world, by looking at business purposes, and banking systems of the future. The second part of this book will cover advanced topics and the contents will get technical. We will discuss step-by-step how Blockchain attributes are working together. Blockchain is based on multiple existing technologies working together, and this book will reveal each of them for your understanding. Reading about each technology explained in this book will get you closer to mastering Blockchain and understand in depth how it improves data integrity, as well as enhances data security. It will then move on to explaining the advantages of terminating trusted third-party services and replacing them with mathematical algorithms and digital signatures. Next, it explains what 100% Data Availability is, using a fully decentralized peer-to-peer network, and how data will always be available. Finishing off,

by explaining Lightning network and how it's going to help us by using faster and cheaper payment transactions, and how employee payments can be made, not daily, but every second.

Book 2

Book 2 will dive into the details of Bitcoin, Bitcoin mining and Blockchain basics, so by the end of this book you become confident to have a decent discussion about any of these topics. First and foremost: What is Bitcoin right? Well, there are many ways to explain what it is, and I heard plenty of versions to be honest. Different people would explain in a different ways, but you really can't describe it one sentence. To explain what Bitcoin is, 5 minutes simply not enough. The Bitcoin industry has been grows and became so big, that even it's one instrument, it described as a completely different asset. Traders look at it one way, investors look at it in another, but same applies to Bitcoin merchants, cryptocurrency exchanges, Bitcoin core developers, journalists, hedge funds, governments or regularity agencies such as SEC, CFTC, or FINZEN. But criminals and underground figures also using bitcoins for different purposes. Generally most people look at it as a medium of exchange, investment, trading asset, or store of value. In order to simplify what Bitcoin is, you might take into the consideration of the following: Bitcoin is a cryptocurrency, also in a category of digital assets. Bitcoin is a revolutionary technology which enables users to send payments over the internet, and because it uses computer hardware for it's network in a decentralized manner, it also known as a peer-to-peer system. As a peer-to-peer system, it has no authority, therefore it can not be easily manipulated or duplicated. Each payment known as a Bitcoin Transaction, and once they are verified, they get recorded on it's ledger system called blockchain. The reason we call the ledger system blockchain is because bitcoin transactions are gathered in a forms of blocks in about every 10 minutes, and because they create a chain of blocks, we began to call it blockchain. The Bitcoin blockchain, known as the ledger system, is open to the public, and every computer which is part of the network has a copy of the ledger. Each of those computers that reside on the network, are also responsible to verify transactions, which they get rewarded new bitcoins from the Bitcoin network.

This process is actually called bitcoin mining, or just mining. To simplify it, mining is nothing but validating bitcoin transactions and getting reward for it from the network. Bitcoin miners are specialised computer hardware, and their main responsibility is to verify transactions. The system has been programmed, so that only 21 million bitcoins will be ever mined, and every 4 years the mining reward decreases. For this reason, it has a predicted supply, and it's governed by scarcity, makes it valued like gold in a digital form. Bitcoin is the first of it's kind, and often people describe it as money of the internet. The bitcoin supply is controlled by computers instead of banks, and this is also the reason once you have some bitcoins, you are your own bank. Anyone who has internet access can use it, and transfer any amount of money anywhere in the world anytime of the day without any intermediary. Bitcoin also known as an efficient accounting system, as it's running automatically, without any human intervention, eliminating trusted third parties. Because the ledger system publically available, every bitcoin is accounted for, therefore it's impossible to counterfeit or duplicate bitcoins on the network. Because if these properties, bitcoin is also known as a trusted payment system, or trusted money. Because the network is not controlled by anyone, there is no central point of failure; therefore it can not be shut down. Bitcoin exist since 2009, and the network has never been hacked. Bitcoin is transferable between 2 parties and can be used anonymously; all though it is not completely anonymous, so the best term to be used is that it is semi-anonymous. The bitcoin ledger contains all previously made transactions, so it's a perfect decentralized accounting system in a human history that was ever created. Bitcoin has many services that people are interested, and One of the first ability that attracted a certain type of people was its decentralized nature. Over time, people began to take advantages of its anonymity and began to use it on the dark web, which wasn't ending well, and its value has decreased, but due to government regulations, bitcoin became legal to be used. In the early days of Bitcoin, the transactions had no fees, therefore another group of people began to take an interest, and started paying employees all over the world, or even used Bitcoin for donation purposes. Due to the continuous use cases, the demand for bitcoin has been grown, and people began to invest or even trade with it. This network effect has made Bitcoin to be even more

visible to the public, and people began to use it as a store of value. At the end of 2017, CME and CBOE also taken a keen interests and started listing Bitcoin Futures, where qualified investors able to place bet on the upcoming price of bitcoin. It is fair to say that Bitcoin is used mainly for store of value, and this is due to its increasing value. As you see there is a huge industry revolving around Bitcoin, continuously making headlines in the media, even not everyone knows exactly what it is, or don't own any, but at least, most people already heard about it. In the following chapter I will dive into more details why Bitcoin can become the money of the future, so I will talk about its origin, and what was intention, or reason for the creation, then explain its main properties, so we can understand how useful is in our current society.

Book 3

Book 3 covers all the public evidences about Satoshi Nakamoto. Satoshi Nakamoto, who invented Bitcoin, also implemented blockchain and deployed the first ever decentralized digital currency, which is known as cryptocurrency. In order for Satoshi to succeed, he had to find a solution for the double-spending problem. The double spending problem relies on easily copied digital files; therefore he created a consensus system that is capable of auditing digital files by eliminating trusted third parties. Just mentioned Bitcoin, blockchain, cryptocurrency and decentralization but if you look around in todays market, you can see and hear different people using these terms for various purposes while trying to separate one from another. For example, large companies love mentioning that they will use the blockchain technology so they will keep all their information or data on the blockchain while they don't mention anything about decentralization. Many entrepreneurs and new fin-tech companies continuously creating new digital currencies, which they dare to call cryptocurrency while they use terms like blockchain, but the large percentage of these cryptocurrencies are not decentralized or fairy mined. This makes them a scam token or scam ICO. A centralized digital currency. Still, there are others who truly believe in Bitcoin and know that implementing blockchain without decentralization has no meaning and there is only one true cryptocurrency out there that was fairly mined and distributed from the beginning with no pre-sale involved such as

every ICO nowadays. There was no money collection for the development and that project has grown to be the most decentralized blockchain which is of course the Bitcoin network. Those who love the idea of decentralized blockchain or fairly distributed cryptocurrency like Bitcoin love to talk about it and often spread the word to others yet all we see is an opportunity. These opportunities revolving around investing, trading, running online or offline exchanges, creating cryptocurrency Wallets or other related applications, writing books about these topics, creating documentaries, or video courses but the main focus always stays the same; Opportunity. A chance, a prospect, a break to spread the word. Yet most of these topics always seem to revolve around Bitcoin, blockchain, cryptocurrency, investing, trading, HODL-ing, BTM-s, ICO-s, pump and dumps but very few people talk about the inventor. The fact is that most people in crypto have no idea who invented Bitcoin or blockchain and the first ever decentralized cryptocurrency. Some might say, “ohh yeah I think it was some Japanese guy right?” Others might say “Bitcon is a scam!” In fact, even heard people saying that Bitcoin was created by the NSA. Found some great resources which include documentaries, books, audiobooks and courses on these topics, still, even the best contents out there don’t focus on the inventor of Bitcoin more than 5 or 10 %. Therefore it was time to create a book that is purely focusing of the architect of Bitcoin. There is a cryptocurrency revolution out there. There are thousands of cryptocurrencies exist (7671 to be precise in November 2020), which are now reachable for investors in every country around the globe. There are over 30 thousands of online exchanges (32933 to be exact in November 2020), as well thousands of cryptocurrency wallets including online wallets, desktop wallets, mobile wallets, hardware wallets and paper wallets. Bitcoin futures listed on CME (Chicago Mercantile Exchange) and CBOE (Chicago Board Options Exchange) for traders, which is completely legit and approved by the SEC (U.S. Securities and Exchange Commission). We also have Grayscale Bitcoin Investment Trust aka GBTC which can be utilized as a saving account which I believe the only S.E.C. approved trust that can be used as a retirement fund. GBTC also has an advantage of quarterly withdrawable dividends. There are Bitcoin and Blockchain consultants, Bitcoin day traders or even Bitcoin brokers. There is also a huge demand for blockchain

application developers, sales people and marketers. There are Bitcoin related certifications such as Certified Bitcoin Professional, Certified Bitcoin Expert or Certified Ethereum Developer. Likewise there is a huge demand for Bitcoin ASIC miners, sold by multiple companies such as Halong Mining, BitFury, Canon or Bitmain and many more. There are Bitcoin cloud mining contracts, Bitcoin ATM-s, Bitcoin Vending Machines, Bitcoin algorithmic trading software or Bitcoin bot traders and many of them acting as a built-in feature on multiple cryptocurrency online exchanges. There are thousands of Bitcoin news channels, forums, Facebook groups, Twitter fans and real time meet-ups all over the world in multiple languages. You can accept Bitcoin as a merchant or make purchases using Bitcoin or other cryptocurrencies. You can buy literally anything on thousands of websites. There is also a never ending Bitcoin related gift items available such as T-shirts, hats, watches, bracelets, key rings, mugs, pens and so on. As you see the Bitcoin industry has been grown dramatically after a decade of its existence, but we must not forget it was all started with a mystery man called Satoshi Nakamoto. Who is he, or she, or they? What kind of personality or political believes he has? How about his writing styles or technical expertise such as coding skills, cryptography, game theory framework or financial education? Well, this book will cover all that. This book will focus on the mystery man, how it's all started, his adventures and how he managed to stay anonymous for over a decade.

Book 4

Book 4 mainly focuses on cryptocurrency wallets, but you will also learn how to buy bitcoins and other cryptocurrencies from multiple online exchanges. You will also learn how to transfer cryptocurrencies from hot wallets to hardware wallets, so by the end of this book you will able to confidently create your own wallet, including paper wallet, online wallet, desktop wallet or mobile wallet and start investing in Bitcoin or other cryptocurrencies. Furthermore, you will learn where to buy the most secured hardware wallets the cheapest price possible, how to install them, and how to make cryptocurrency transactions by either sending or receiving using cold

storage. This book is structured in a way that even if you are a complete beginner you have nothing to worry about, as you will learn all the pros and cons of every single types of wallets, including online wallets, paper wallets, desktop wallets, mobile wallets, and of course the most secured amongst them all; the hardware wallets. First you will learn what the main characteristics of cryptocurrency wallets are and how they work. You will also learn the importance of the cryptocurrency wallet and how a Bitcoin 3D QR code have been supporting a revolution that taken place recently. Next, you will learn some great tips on how to choose the best wallets that suits your requirements, either if you want a wallet because you are a long term hodler' or want to become a cryptocurrency trader. Perhaps you want to run a business and accepting cryptocurrency payments online or offline like a restaurant or shop, or even if you want a wallet to receive your wages or pay your employees' in digital currencies, well, by the end of this book you will learn them all. This is because you will learn how to install hot wallets, desktop wallets, and mobile wallets for free and how to start buying bitcoins right away. You will also comprehend how to exchange between fiat currencies or altcoins, such as ethereum, Litecoin, monero or many others. Then you will understand the details of the most secured hardware wallets and what are the pros and cons of each. Next, you will learn how to buy hardware wallets and what online shops are selling them the cheapest, or which ones are providing the fastest delivery. Next, you will learn how hardware wallets work and what you must be aware in terms of security philosophy. Next, you will learn how to send bitcoins from an online exchange to your own hardware wallet. You will also learn why you must own your private keys, which is a very important topic because there are many cryptocurrency wallets hacks and thousands of people already lost their cryptocurrency portfolio because they have ignored to keep their funds on cold storage. You will also comprehend what is a Man in the middle attack and how hackers can manipulate cryptocurrency transactions, so you will understand how you can avoid being a victim of such attack. Finally, you will be introduced to a list of wallets (30+) which you will be able to utilize in order to find the most suitable wallets according to your requirements. This is the most comprehensive cryptocurrency investment book up to date, which

exclusively focuses on cryptocurrency wallet technology.

Book 5

Book 5 focuses on privacy based cryptocurrencies and reveals the potential ROI or return on investment on the various well known anonymous altcoins. First, we will define anonymity and why privacy based cryptocurrencies are needed. Then we will dive into the details of Privacy focused coins, who wants to use them and how they function. Next, we will look at the current cryptocurrency market and clarify what is Initial Coin Offering, pump and dump, online scam and how to avoid them. Next, you will learn about cryptocurreny basics and the differences between Proof of work and proof of stake algorithm but you will also explore other technologies such as zero knowledge proof and CryptoNote ring signature Algorithm. Next you will learn about 17 different kinds of privacy based cryptocurrencies. We will explore each technology and coin by analysing fundamentals, technical details, trends and their market capitalization and calculate the return on investment. In terms of privacy based cryptocurrencies you will learn a few great strategies on what you should consider before purchasing them, where to buy them, how to buy them and how to sell them. We will look at Komodo, DeepOnion, Solaris, Sumokoin, Firo aka Zcoin, AEON, Bytecoin, Navcoin, PIVX, DASH, Zcash, Monero, Verge, Beam, Grin, Particl and Horizon aka ZenCash. Lastly, we will reveal which privacy based cryptocurrency has the most potential backing it up by various fundamental and technical analysis. Finally, we will cover cryptocurrency regulators such as SEC, CFTC and FinCen. This book is structured in a way that Even if you are a complete beginner, by finishing this book you will become a cryptocurrency pro! This is the most comprehensive cryptocurrency investing book up to date which exclusively focuses on the Privacy Based crypto assets.

Book 6

Book 6 focuses on bitcoin and cryptocurrencies trading and reveals various techniques and strategies. First, we are going to take a look at several

Portfolio Tools that you can chose from such as Blockfolio, Messari, Altpocket, Deltaand Cointracking. Next we are going to cover a few Market Manipulation techniques like Pump and Dump, Order book spoofing, Wash trading, Stop loss hunting and FUD. After that we will take a look at Bitcoin Options, Option Theory and Option Strategies.
Next we will cover How to build options strategies on Deribit and Extensive potential for Option markets. After that, to make your life easier when it comes to TAX, we will cover various Crypto TAX tools such as Crypto Trader TAX tool, Bear.Tax tool , Koinly and CoinTracking. Next, we will look at a few trading formula mistakes such as Stop losses, Overtrading, Analysis Paralysis, Leverage issues, Bad Broker Advice, Choosing the wrong Exchange and Overconfidence. In terms of Market research, we will look at Market Activity & Initial Research, Technical Elements,
Source Code, Upgrades and Roadmaps. Following that you will learn about the Crypto Market Cycles, the Dynamics between Bitcoin and altcoins, Tokenomics, Technical Indicators and a successful Exit Strategy.
Next, we will cover Crypto Exchanges and look at the pros and cons of each such as Coinbase Pro, Uniswap, Binance and FTX. After that you will about Leveraged Trading Strategies, BitMEX & BTC Futures. Lastly, we will take a look at how Exchanges make money and how to use leverage responsibly.

Book 7

Book 7 focuses on bitcoin and cryptocurrencies trading and reveals various techniques and strategies. First, we are going to take a look at Margin Trading Features, Lending, Borrowing and Spot Trading Step-by-step on dYdX. After that, we will take a look at how Trading BOTs operate such as TradeSanta, Shrimpy, Gunbot, Crypto Hopper and 3commas. Next, we are going to look at Key metrics signals & Red flags, Volume, Liquidity and Artificial Perception of Demand. Next, you will learn about Trading tools such as Interest earning tool, a VISA Cash back Card on Crypto.com. Next, you will learn step by step how to do a 100x Altcoin Research. Here, you will learn about Screening Process, Trading Volume & Exchange activity. You

will also learn how to identify Onchain Metrics, Development Activity, Project Uniqueness, Adoption & Community Support. Next, you will learn about Trading Tips such as Option Moneyness, Put Call Ratio, Options Skew, Market Parameters and Options Expiry Dates. Moving on, you will learn about Bullish Candlestick Patterns, Bearish Candlestick Patterns and Continuation Candlestick Patterns. After that, we will comprehend what is Implied Volatility, why Implied Volatility is Important and what is an Implied Volatility Rank. Next, you will learn about Trading Psychology such as Gambler's Fallacy, Confirmation Bias, The law of Small Numbers, The Survivorship Bias, Correlation, Hindsight Bias, Recency & Attribution Bias and Sung Cost Fallacy. After that, you will learn what separates Winning traders from Loosing Traders. Lastly, you will how to create a Step by step checklist for a Trading Plan and how to set up a Trade Order. If you are ready to jump on board, let’s begin by looking at dYdX Margin Trading Features.

BOOK 1

BITCOIN IS BLOCKHCAIN
AND HERE IS WHY!

LEARN FAST HOW
BITCOIN, BITCOIN MINING AND BLOCKCHAIN
TECHNOLOGY WORKS

BORIS WEISER

Chapter 1 How Blockchain is connected to Bitcoin

Before I begin to explain to you what Blockchain is, first, I would like to touch on Bitcoin, as there is a myth going around that Bitcoin equals Blockchain. Well, that is incorrect. Though, it is often referred to as the same thing. Bitcoin is cryptocurrency, digitized money, that is allowed and kept alive due to the technology called Blockchain. When Blockchain technology began to exist, the first application that was tested on the platform was Bitcoin. Because Bitcoin was the first application on the Blockchain technology, one might say that Bitcoin is Blockchain, and that could make sense. However, Blockchain is not Bitcoin. I hope that makes sense. Blockchain is so complex that still there are very few human beings who understand each part of it. In fact, Blockchain is so complicated that we (as humans) keep on finding more and more ideas that this technology can solve every day. We could say that Blockchain is solving problems. Nevertheless, for some large Financial Organizations, it's causing certain issues. Some of these matters are getting addressed, and if you keep up with the news, you realize that more and more companies are beginning to use Blockchain Technology for many purposes. The Blockchain is truly revolutionary, as it's not for solving just one issue for some people, but can fix many problems for everyone. It has re-invented the financial institution, and the proof of that is simply because Blockchain is running and has existed for 12 years already, beginning in 2008. The Blockchain is a globally distributed database that is completely decentralized, meaning it has no boss, or someone that we could blame or award. It is running on all computers, and it's unstoppable. The Blockchain is built up from multiple blocks that are un-replaceable. Therefore its chain system represents the single source of truth. Once there is a new block created and added to the existing Blockchain, it replicates itself on its system, which resides on the internet, then just synchronizes the same details on all the computers that are running B lockchain. This replication is what makes it un-replaceable. Therefore, it provides full transparency in all administration. Because there is no human intervention in the process of adding and further expanding when new blocks are created every 10 minutes, it exhibits an efficiency that no person has ever achieved. Because each time a new block becomes visible on all computers in the world, it allows full accessibility to all human beings. Where Blockchain stands right now, I mean

in 2020, is more like where the internet was in 1993-1995. What happened back then is most people said, “its nonsense,” or “what’s the point of it?” Granted, at the early age of the internet, there were only a few personal computers, very few websites and the network was slow. In fact, it was so slow that if you wanted to download a one-page PDF document, you would probably go out for lunch, come back and you still had to wait another 20 minutes. The internet (Interconnected networks) seemed like a dumb idea to most people, even for those that had power in politics or others that already had existing large retail infrastructure. They believed that it was just background noise. Slowly, the internet grew and became bigger and faster. And once local support opened on the internet, everything changed. When you think about Blockchain, don’t assume that it will not have the same power. Currently, we are innovating in large scale and technology grows with such a high speed that no human can keep up with it. Blockchain will change that dramatically, so instead of continuing to talk about the future, let’s take a step back and understand the history of finance.

Chapter 2 A brief history of finance

The purpose of this chapter is to understand the innovation of our existence. Therefore, let's take a step back a few hundred years. Trading has always been present in our lives, as it is mandatory for our food chain, and probably will never go away. When you take a closer look at the basic human needs for survival, you quickly realize that the three most important requirements are air, water and food. Because air and water can be found in many locations for free, I will take an example of food and start to analyse it in further detail. Food items have been identified since the early ages as one of the primary human needs for survival. Therefore, we have understood that food has tremendous value. Like anything else that has value, it became part of the global trading chain, and it was one of the first early paying methods amongst humans in exchange for particular goods or services provided. Because food has always helped for basic survival, it was one of the best paying methods for an extended period. In fact, there are many locations existing in the world that still use this approach at present. As civilization has moved on, especially with more developed villages and cities, methods of payments have begun to change. Back then we had no freezers, or fridges, and using payments such as food items like exotic fruits or any meat just went to waste. This caused lots of issues. Therefore, this problem had to be resolved. The solution was a new type of payment method, something that wouldn't easily rot or waste. Nevertheless, had to be exchangeable for food or any other goods or services. Shiny metals were introduced to the world as a new payment method, and such were silver or gold. Most people didn't like the idea at first. Still, it was implemented, and slowly it was accepted widely. It was exchangeable for food items, and other goods or services and it was truly revolutionary, and still today, when you look at the silver or gold value, they are continuously increasing. Humans have realized that it is getting much harder to mine gold and silver. Hence, precious metal had to be discontinued as the major payment currency. The introduction of paper money seemed silly, since as humans, we are uncomfortable with change and we are hesitant to adapt to anything that we don't understand – at least at first. After a while, all sorts of paper money was implemented in a centralized form, nearly every country in the world. The new payment method of paper money was alive and booming all over the globe. Paper money is OK, but we could mention

countless countries where paper money has failed again and again due to its value decrease in long term. The reduction in value of paper money has other roots too, such as easily counterfeited in large scale. Additionally, like anything else in the world, we have learned that goods with limited supply have an increase in value, especially in the long term. Conversely, the opposite happens when paper money keeps on getting printed, decreasing in value. When it comes to paper money, it's a fascinating topic. The fact that we have learned, on various occasions, that paper money is a failure, we keep on re-inventing new ones. We believe, this time, it will be a success. Look at the example of the Euro that has taken over currencies such as; German Mark, French Franc, Italian Lira, Dutch Guilder, Spanish Peseta, Slovak Koruna, Austrian Schilling, Maltese Lira, Finnish Markka, Greek Drachma and more to come. It appears paper money is still going to be present for a while. However, before jumping ahead, we had another currency introduced after the paper form in our new digital world called SWIFT. SWIFT stands for Society for Worldwide Interbank Financial Telecommunication It began in 1973, and this newly created network now enabled all the financial institutions to transfer secured financial transactions in a reliable environment across the globe. This idea was, again, truly revolutionary. Using the internet to make payments is very helpful, not to mention, that nowadays using contactless cards is just extremely comfortable. The speed of implementation, when making payments, becomes very fast. When you are looking at an international bank transaction it might take 3-5 days, but you can do this using your laptop at your home or your mobile device, anywhere. But at first – when it was introduced – it seemed alien and most people didn't believe that it would ever work. Slowly, we have learned that certain payments can be automated: such as paying your bills or a service that you have subscribed, and of course, most large companies are now paying all their employees through bank transfers. Well, there are still many companies who pay their employees cash in hand, as they don't wish to pay taxes. These companies choose to remain anonymous instead of sharing with the banks all their assets for various reasons. As always, people had to adapt. The idea that all your wealth is contained on a piece of plastic card was daunting. The world of payment has yet changed again. Centralized banks have scaled, and they have introduced many different systems that one may choose. Some of the most known of virtual payment methods are; Visa Debit, Debit Card, Credit Card and ATM machines. Due to the dot-com boom and the revolution of the

internet, other digital payment methods were introduced by various third-party companies, providing additional secure transactions for a particular fee in exchange. Although higher priced, we have now reached the point of enabling international operations with people or companies that we never have to talk to or see. Even if we were to have a problem trusting a business or particular goods; we could still proceed to make transactions, due to the third party that guarantees the payment will be only completed once goods have arrived as described. For example, you make a payment for an individual product using PayPal, simply because you know that, worst case, you can ask for a refund and PayPal will help you out—making sure that you get your refund if the goods or services are not as described when you placed an order. Such well known centralized financial systems are; PayPal, Payoneer, Alipay, eCash and there are many more. In 2008 there was a new currency introduced, but this time it was something very different. It was the first digital currency, called Bitcoin. It was not introduced by a well-known company or bank, neither any government, but in a software form—running on the protocol called Blockchain. As always, not many people were interested in adopting it at first; they didn't understand its purpose. It might require a bit of research to understand. We know that cash works and that many other currencies exist. We can make payments using our bank cards, and so many other options, when it comes to making a payment—so why bother, right? Well, Bitcoin was the first digital currency that was introduced. However, as of November, 2020 there are more than 7600 different types of digital currencies that exist. What does it mean to us now? I have friends that don't work in the IT Industry, and when I asked them about Bitcoin or cryptocurrencies, they frequently look at me like I'm speaking in a foreign language. The reality is, that although some might have heard of cryptocurrencies, they still never bother to investigate the potentials—and how much it can, and will, form our future. What I am trying to tell you is that when looking back in time and analysing the history of financial institutions, you may realize that the form of payments has significantly decreased from their physical value. They not only become smaller, lighter, or thinner, but more virtualized, and now to the point where we, people, don't even have to make them — as the digital currencies are running on our current internet (interconnected networks).

Chapter 3 Bitcoin fundamentals

Bitcoin is the first known digital currency that is running on a technology called Blockchain. It is entirely decentralized. Therefore, no one has control over it. It also is known as electronic money or digital currency. Though, it is a peer-peer payment system. Consequently, it's software. It has no real presence whatsoever, as it's growing on your computer's hard drive. In fact, on every computer that exists in the world. This currency will never be touched by anyone as it only exists in a digital form. Regards to its value, it does seem to fluctuate. Nevertheless, it has kept itself steady for a long period: moreover, continuously increasing. Back in 2008, it began to compete with the dollar—when one Bitcoin was equal to 0.05 dollars. But, in December 2017, one Bitcoin has reached $19,497; its highest value as of yet. Over the years, Bitcoin not only proved that it could reach its highest over and over again, but it has increased its value higher than what we have ever experienced with any other currency. We will keep on seeing Bitcoin's increase in value, especially around each four year mark. Why would I say that? Well, let's just say that I have my reasons. How many Bitcoins are out there? Good question and you can calculate it yourself. Of course, it all depends on the date and time you're reading this book. So, let's look at some of the facts that we know for sure before beginning any complex calculations. The first 50 Bitcoins were created on the 31st of October 2008. Then, 50 more Bitcoins were created every 10 minutes until 2012. After 2012, the amount of Bitcoin production reduced to half—meaning every 10 minutes, 25 new Bitcoins were created until 2016. Since 2016, the process has followed the same principles—meaning, every 10 minutes, 12.5 Bitcoins was created until 2020. Since 2020, we are creating 6.25 Bitcoins until 2024. This process will keep on going until 2140, until there will be 21 million Bitcoins on the market. If you want to know the exact dates when the next drop will happen, I recommend you to check out the following website: https://www.Bitcoinblockhalf.com/

Moving on, let's discuss some of the bad reputation of Bitcoin. In case you haven't heard of the Dark Web, let me explain a little about it. I could dedicate a whole book for the Dark Web, and I might in the future. I am not interested in trading drugs or guns online. Just because that is a list of things that can be purchased on the Dark Web, does not mean I will ever be

participating in those markets. What you must understand, is that the Internet as we know it—through search engines like google, yahoo, or bing — isn't the only web out there. There is another, and it's known as the dark net; it can be reached through another search engine called TOR. TOR network is also known as an onion router or onion network. TOR is capable of hiding the IP Address of the end user; therefore, making whatever is done on the internet completely untraceable. Even your internet service provider wouldn't know what website you visited, except that you have visited the TOR network. You might look around and see for yourself, what kind of services is offered there, but it's up to you. I have visited the dark web before to get a feel for it, and the more you look around, the more you will find ugly services. And I am sorry to mention these, but the things I have seen are disgusting, and for those who can be easily upset, I would not recommend it at all. My point is that the guns and drugs traders on Tor ask for payment in the form of Bitcoin. Bitcoin is untraceable, as well as the TOR network. Therefore, the Dark Web is a haven for criminals. Do criminals use Bitcoin too? They sure do. In fact, they have no other choice when it comes to illegal goods or services online. Before you close this book and walk away from the idea of using Bitcoin because criminals are using it too, please think twice. Bitcoin wasn't created for criminals. Bitcoin was designed for everyone, and please don't forget about those 3 billion people that Bitcoin can save when it comes to financing. Another issue that happens over and over, is Bitcoin accounts get hacked, and people are left with empty wallets. Please don't misunderstand this point. It's not the Bitcoin that is hacked, but the end-user level victim's Computers, or mobile devices. The value of Bitcoin has become enormous; and hackers do educate themselves too. Therefore, they have changed their game once again, and realized that hacking Bitcoin accounts is profitable and untraceable; so, why not do it—especially do it on a grand scale? This issue has been addressed, and if you decide to own a wallet, you must make sure that you always back up your wallet, as well, always have all the security features enabled. Some of these security features are like 2-step authentications that don't require much learning or time, still, better to be secured then assuming that hackers will never find you. So, because many people have fallen victim to Bitcoin account hacks, they have stopped trading or investing in Bitcoin or any digital cryptocurrency. You might be familiar with the website WikiLeaks — a non-profit organization responsible for publishing secrets and classified information anonymously. Individual governments are not

happy with the website and they have issued the site to be shut down. The site requires basic maintenance, as well as security, and the only contributors able to help have had to use Bitcoin. As a result, the website has stayed alive to this day. This is one of the most famous examples. However, there are countless causes that people have been able to provide help to others, even to the other side of the planet, using Bitcoin. The most common speculations and accusations against Bitcoin are its possible fluctuation. Why is that? Well, people often say, “What if there is another type of cryptocurrency that could compete with Bitcoin using the same underlying technology, the Blockchain? Would Bitcoin lose its value?” The accusations are indeed possible, but looking at the history of Bitcoin value, only significant increases happened, even with 7600 other cryptocurrencies. I am not a futurist, but after analysing the facts, I think it’s fair to say, that the Bitcoin is on the rise, and will not stop for a long time. To learn exactly how many cryptocurrencies are exist up to date, I recommend you to check out the following website: https://coinmarketcap.com/

Moving on, you might ask; what can you purchase using Bitcoin? Well, you can buy anything on the dark web — of course — I do not recommend that, as you might come across criminals who would try to steal or hack into your Bitcoin wallet. Some cyber criminals would even try to blackmail you. If you do not provide your details, you should be just fine. Realistically, more services are excepting Bitcoin, such as Hotels, Restaurants, Coffee shops, even some takeaway shops are now offering payment method using Bitcoin. Large retail companies are also accepting Bitcoin, such as Shopify, TigerDirect, and many more. To see how wide ranges it can be already, you have to look around where you live. The big cities have all sort of offerings, such as Taxi Service, Hotel Industry, Bicycle rent, Car rents, Private Jets, Pubs and son on. Also, you may consider other large companies that are now accepting Bitcoin, such as Dell, Microsoft, Zynga, Reddit, Wordpress, Subway, Expedia.com, Virgin Galactic, OK Cupip, Stream, Alza, Lionsgate Films, Badoo and many more. By using Gift cards, multiple applications also allow customers to purchase on websites, such as Amazon, Walmart, Target, Nike, GAP, Sears, Papa Johns, Best Buy, iTunen, eBay, Starbucks, Zappos, HOME depot and many more. I wanted you to see that some of the largest companies are already adapting to the idea of accepting Bitcoin. Furthermore, to understand the range of goods and services that can be purchased, please see the list of categories that you may choose from: Airline, Automotive,

Beauty, Clothing, Department Stores, e-Commerce, Electronics, Gas, Gifts and Toys, Grocery, Health, Home and Garden, Home improvement, Hotel, Jewelry, Movies, Pets, Restaurants, Shoes, Sporting goods and more. As you see, the categories keep on growing, and if you are more interested in what stores you can pay using Bitcoin, you might check what you have nearby you, or what online platforms can deliver to your area. Another great website I recommend for you to check is called: https://coinmap.org/view/#/world

Moving on, you might ask; how comes not everyone using Bitcoin? Well, the reality is that most people who are already aware of the existence of Bitcoin, are too lazy to do some research for better understanding of the potentials. Personally, I first heard about Bitcoin in 2014, and I didn't look at it that much. What I understood, was that Bitcoin was some form of online payment method, and mostly criminals were using it because it's untraceable. That's it. I keep up with the news, and somehow, no one seems to talk about it unless there is a significant Cyberattack, and the hackers would demand ransom, or some payment in the form of Bitcoin. Anyhow, at the end of 2015, I heard about Bitcoin again so I mentioned it to my friend Jack. He said that, yes, he was aware of Bitcoin and its worth was like $300. When Jack told me how much it worth at the time, I couldn't believe that one Bitcoin was worth $300. I still didn't understand what Bitcoin was. I supposed that it was like a real physical coin, I still had no clue that it only exists in a digital form. Then another friend Steve, who overheard what we were talking about, said that he couldn't believe that I had never heard of Bitcoin before! So, I said, "Yes, I did hear about it, but I didn't know that it's worth so much." I started thinking more and more about it, and I began to do some research. A little later, I had an idea to make Bitcoin using my old laptop! So, I told Steve and Jack that I heard that computers could generate Bitcoin, and if it's worth like $300 each, I might be able to produce one or 2 every week. Clearly, I had no clue what I was talking about, and they told me off that it's not that easy. However, they couldn't explain it to me, how it's exactly done. They said that Bitcoin it's for criminals. But I stated that it sounds like an exciting technology. They replied; "OK, so why do you need Bitcoin? What do you want to buy? Do you want to buy something on the dark web?" They made me speechless, so I stopped talking about it. Still, I secretly begin to learn as much as possible about Bitcoin and of course that lead me to another interesting technology called Blockchain. My point is, that most people have been misled by fake news, and for those that might be interested, it takes a

long time to understand how Bitcoin or Blockchain works. Therefore, most people give up research, and will not get involved in any way.

Chapter 4 The Publication of Whitepaper

Lehman Brothers collapsed on the 15th of September 2008. The largest bankruptcy that has ever happened in US history occurred. Lehman Brothers was operating in other countries too, and the outcome of that day was no different anywhere else. Following Lehman Brothers, there were many more Banks and Financial Institutions that had no choice but administration. For months, every news channel was full of the latest stories that another large company had lost all its assets, again and again. At the same time, unemployment began to rise, and then slowly, lots of people started losing their homes due to uncompleted payments. Most of the small businesses had to shut down. There were fewer customers in the restaurant, and people were thinking twice before spending money on anything. The financial crash caused plenty of misery, and not only in the US or the UK, but many other countries too, that are still in a state of recession ever since. Property prices began to drop, and finding a new job wasn't easy, even overqualified people were applying for jobs everywhere. There were not enough job vacancies to fill the increasing demand. Most people were following the news — which is most of the time is manipulated and it's only purpose to create drama and fear amongst hard working people. Controlling the media is an excellent way to manipulate people, their beliefs, and freedom. Using media — such as news channels and newspapers — to reach people, is indeed one of the best ways create slaves, by making them believe that the world is exactly what the media is providing. Just think about an average day when you meet like 10 people. Someone, if not many of them, will tell you a story that starts like this, "Did you hear about (XYZ)" Next, someone else will ask, "Where did you hear that?" The answer will be similar to something like this, "I heard it on XYZ news channel, or in the news, or read it in the XYZ newspaper." Everything is such big news for days, sometimes for weeks, then suddenly — all is forgotten. How come? Funny enough, around the same time, in an unfrequented online forum, a paper was posted to a cryptography mailing list on metzdown.com, titled as: "Bitcoin". The subtitle was: "A Peer-to-peer Electronic Cash System". So, what's that? It's not from the CNN, or BBC, NBC, CNBC, or whatever you name it news channel. Therefore, it must be nonsense, right? Yeah, it's most likely fake news, and whatever it is, it seems too complicated. Therefore, it didn't pique anyone's interest. This white

paper was published in October 2008, less than two months after the biggest financial crash in history. The author named himself Satoshi Nakamoto and explained a couple of points related to this new digital currency called Bitcoin. He stated, that he believed he had found the solution for the biggest issue that we face and he called the technology Blockchain. Also, he explained not only how it works, but that this system has already been created and is running in a software form using the current internet as its platform. There are many speculations about this, and you might find multiple answers about what exactly happened; the most important among those are — why now? How come such a serious document was published just after the largest financial crash in history? Well, we might find out someday soon, but the possibility remains that we may never know what triggered the Blockchain technology to be born.

Note:

You can check out the original publication of the Bitcoin Whitepaper on the following website:

https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

Also, if you are interested reading of the full paper, you can read it or download it here:

https://bitcoin.org/bitcoin.pdf

Chapter 5 The Author of the Bitcoin Whitepaper

This book has been written in the end of 2020. Therefore, by the time you are reading this book, it's possible that new light might be shed on who Satoshi Nakamoto is. With the current knowledge at hand, let's try to understand who Satoshi Nakamoto is. First of all, Satoshi Nakamoto is an inventor of Bitcoin, as well the Blockchain technology. All through it's a false name; this is how he introduced himself to the internet. It is a men's name. Nevertheless, it is possible the Satoshi Nakamoto might be a woman. This is one of the biggest mysteries in the technology world. Yet, most people don't want to know exactly who Satoshi is; nevertheless, they are thankful for the technology he created. Unfortunately, many people think that because Satoshi Nakamoto has invented Bitcoin and the Blockchain technology, he is also the owner of those too. The reality is that Satoshi Nakamoto has no control over the Blockchain —neither Bitcoin; therefore, it really doesn't matter who Satoshi Nakamoto is. But we still want to know who is behind the curtains; so, let's think about it again. Satoshi Nakamoto is reasonably a man or a woman—of course—he could be a couple, a group of people, or even a group of women for all we know. Satoshi Nakamoto might be ten people together, but also could be a massive team of 100 individuals. Satoshi Nakamoto might be a child, or he could be old men. Satoshi Nakamoto might have died right after he released his white paper; therefore, he had no time to show his real face. I do understand if you are getting bored of these accusations, so let's begin thinking in a different perspective. Satoshi Nakamoto might not even be human. Well, you might think of me being over the limit. However, it's just so odd that we couldn't figure out who Satoshi Nakamoto is in the past decade; not where he resided, but who he is—honestly—we have no idea. Someone might know exactly who he is. Still, there is no confirmation that would ever have enough evidence to prove who Satoshi is. Back in the day, some sci-fi stories featured individual objects, or tools that we might use in the future, and some that we've already been using for years. I don't want to get into too many specifics; however, think about facetime talk back in the 80's. It was a concept that one day we might be able to do that. And nowadays Skype and Facebook Video Chat is in our daily lives. In fact, there are millions of people connected and capable of being on skype video chat for hours, using our cell phones. The first iPhone was created and launched to

the market in 2007. Since, we have gone through some dramatic changes, and the next decade will be even more impressive. We have received a technology called Blockchain from an unknown person—or I should say from an anonymous source—that will change our world dramatically! I am not suggesting that there are Aliens out there, but I can't deny it either. What I can tell you is that IT Professionals, Software Developers, Experience Programmers, even Cybersecurity Experts are fascinated by this technology, and often refer to it as an alien technology.' The Blockchain is huge, and it certainly takes months, if not years, to fully understand its technical details, and how it fits together. Another thing is that, more and more often, it is said that this technology is just too complex for one man to build. Therefore, there is no way that Satoshi Nakamoto was working on it alone. So back to the million-dollar question, "Who is Satoshi Nakamoto?" Let's look at some of the claims over the years so that you can decide for yourself. What you have to understand is that Satoshi Nakamoto went silent in 2009, and remained like that for the next five years, or at least on the forum where he previously posted and was always active. Supposedly, Satoshi Nakamoto was a 41-year-old man at the time of the publication of the Bitcoin white paper. He is from Japan. However, the first code that was written for the Blockchain was drafted in English that is so perfect; it just wouldn't make sense for a Japanese man to write like that. It would indicate that he must have hired someone, or was working with someone, who speaks and writes perfect English to write the code. In 2014 there were a few newspapers that began to write about Dorian Nakamoto, who at the time lived in the United States in California. Dorian's birth name was Satoshi. Additionally, other circumstances would make him appear to be a real inventor of Blockchain. Apparently, the first reporter who wanted to reach him, asked him, in the form of an e-mail, if he had anything to do with Bitcoin. The response from Dorian was the following:

"I am no longer involved in that, and I cannot discuss it. It's been turned over to other people. They are in charge of it now. I no longer have any connection.''

That was suspicious, and reporters were all over Dorian's house in California. After realizing that it was very serious, he looked at his e-mail again, and tried to explain himself. First, he has denied any involvement in regards to Bitcoin. In fact, he said that he had no clue what Bitcoin is until his son told

him about the news, so he looked it up on the internet. He also went public and explained the following:

“I have nothing to do with Bitcoin. Nothing to do with developing. I was just an engineer, doing something else. If you look at the time spent in 2001, I wasn’t there. I was working for the Government through a contracting company. I just believe that somebody just put that fictitious name in there.’’

There were also published documents on that he has been doing classified work for the United States Government, as well the United States Military. He also has signed documents that he could not be allowed to admit any involvement in his previous works regards to secret projects. After this event, there was an unexpected message on a P2P forum where the Real Satoshi Nakamoto used to post after five years of silence.

“I am not Dorian Nakamoto.’’

Moving on, Craig Wright, who is a well-known Australian Businessman, in 2015 became a next possible man who just might be the real Satoshi Nakamoto. From an anonymous source, documents had begun to leak about Craig Wright to Wired magazine. Most of them had some evidence that seemed as if Craig Wright might be Satoshi himself. One of them, released back in August 2008, Craig himself has stated that he is thinking about releasing a Cryptocurrency paper. Craig become a very attractive candidate for the original white paper that was published by Satoshi Nakamoto and was released in October 2008, just a month after. Another leak, that was also issued by Wired magazine, was another statement by Craig Wright, but this one as dated back to January 2009. This time he wrote that the Bitcoin is about to launch. Indeed, it was January 2009 when the first Bitcoin began to operate. Additionally, Wired magazine also stated that they had received several e-mails and transcripts that collaborate the link.

“There is a leaked message from Wright to his lawyer dated June 2008 in which Wright imagines a P2P distributed ledger.’’

There were many leaks in regard to Craig Wright, especially in the Wired magazine. However, it all changed in May 2016. Craig Wright has stated on his blog that he is now willing to admit publicly that he is Satoshi Nakamoto. This was another turning point; but people have remained sceptical. Two days later Craig wrote on his blog that finally, he would release a series of pieces that will lay the foundation for his extraordinary claim. Even though,

instead of providing evidence, Craig has replaced that post with the following:

“I am Sorry I believed that I could do this. I felt that I could put the years of anonymity and hide behind me. But the events of this week unfolded, and I prepared to publish the proof of access to the earliest keys, I broke. I do not have courage. I cannot.

When the rumors began, my qualifications and character were attacked. When those allegations were proven false, new claims have already started. I know that this weakness will cause considerable damage to those that have supported me, and particularly Jon Matonis, and Gavin Andersen. I can only hope that their honor and credibility is not irreparably tainted by my actions. They were not deceived, but I know that the world will never believe that now. I can only say I’m sorry.

And goodbye.’’

Because Craig has not provided any evidence that he is the real Satoshi, the Bitcoin community has painted him as a liar. Next, was another fantastic action from Craig. He asked the BBC for an interview. He then explained that he is Satoshi Nakamoto, and he invented Bitcoin. Craig also stated that he would not accept any prize or award for this creation, as he is not interested in money or anything from anyone, and certainly doesn’t require any help from anyone. When the reporter questioned him why he was hiding for all those years and how come he has identified himself just now, he had a relatively simple answer. Craig said that he didn’t decide to confront the cameras, as he has people who chose this for him, which, he is not happy at the current present, as this situation will hurt many of his friends and family, as well as his staff members. Next, the reporter asked him what he wanted with the concept of being the creator of Bitcoin, but his answer was that he doesn’t want anything, just to carry on working on his projects. Craig explained that because he has created Bitcoin, or published a document for free publicly, so that he can help people, it does not mean that he should become a well-known star, and certainly no one should force him to admit what projects he is working on. Then he added that he was the main person behind the creation of Bitcoin. But, he had help finalizing it. Next, the reporter pointed out something that most people are interested about. As the inventor of Bitcoin, Craig must have that 5% of all Bitcoin that was saved,

and that is a huge amount of money. As anytime when traders are selling Bitcoin for the dollar, the value of the Bitcoin drops. However, as the inventor has so much of it, there is a fear that if the designer would sell all that when the price is high, the Bitcoin would probably fluctuate. So next, the reporter asked him how much Bitcoin does he have, and how much has he deployed so far. Craig only answered that it doesn't matter how much he has, instead what matters is when will he actually deploy them. Then Craig finished his speech by explaining that he knows that some people will believe him, and some will not, but he does not care, because he will never be in front of the camera. The reality is that Craig is very convincing and, personally, I don't know what to say. I won't judge him or Dorian, but the world we live in is certainly strange for sure. Just think about it. First, we expect someone who claims no involvement whatsoever, and then we find a man who admits that he is him, and we don't believe him. It sounds like we are never going to find out who the real Satoshi is, right? Craig has demonstrated how he started the first Bitcoin transaction. However, he only allowed one person to see it, and that was a reporter who has no technical knowledge. Average tech gurus are not convinced. Also, Craig has claimed that he never wanted to come out and be in front of the cameras. Still, now that he did it—claimed that he is the real Satoshi—he tops it off with providing evidence that he made the first Bitcoin transaction and has options on how he should demonstrate that proof. One right way to do it, is to have someone like a Bitcoin expert see it, who could also verify that he is not lying. His way is a bit fake, as no one can confirm 100% that he is really who he claims he is. So, what's the point? Well, some people have been speculating that if Craig claimed the title of Satoshi, the real Satoshi would be sending a message in some form so he could be tracked down. However, there has been no news ever since from the real Satoshi, like in the case of Dorian. When you think about it, if you were, secretly, one of the wealthiest men on earth, would you go to the BBC and tell this to the World? Speaking to the World does not just entail being popular in front of average people, it puts Craig at risk, right away, of being targeted by Cybercriminals and Black hat hackers. It's so simple that anyone would understand it immediately. So, when you're thinking about someone who is genius enough to implement a technology that will change, in fact already changing the world, wouldn't you think about Hackers? Most IT Professionals just aren't convinced enough; therefore, the question remains about who the Real Satoshi Nakamoto is.

Some people believe the genius behind the Blockchain technology is Craig; some believe it's Dorian. However, most people from the Bitcoin community don't think that any of them has anything to do with Bitcoin or Blockchain. In fact, 70-80% of people believe various other possibilities, so let me explain some of them for you.

According to certain researchers, one of the biggest theories is that Nick Szabo may have written the Bitcoin white paper. When they compared more than ten possible people who might have anything to do with Bitcoin's creation, Szabo's published writings were the closest, linguistically, to the original white paper that was published by Satoshi Nakamoto. Nick Szabo is a computer scientist; in addition, he is also an excellent cryptographer and well-known Bitcoin expert. Additionally, he is famous for his speeches in regard to Blockchain technology, digital currencies, and smart contracts. Many people have interests in any of these topics. Especially, well known speakers about Blockchain or Bitcoin. However, not many people are aware of what some of these so-called experts did before the birth of Bitcoin. On the other hand, Nick Szabo had an idea about a decentralized digital currency back in 1998 that he called "Bit Gold." What a coincidence, right? Nick didn't only have the idea, but he also developed a mechanism for it, and eventually created, the Bit Gold. Nick did not post on his blogs every day. In fact, he wasn't known to publish anything: but when Bitcoin was created, back in 2008—just two months after the official release of Bitcoin—Nick began to write about Bit Gold in more depth. There actually isn't much known about him, an excellent example is that Nick's date of birth has not even been confirmed by anyone so far, and because of this, other curious people have begun to investigate Nick even further. According to Wikipedia, Nick was a law professor at George Washington University; but after contacting the University, they found no record of anyone with the name Nick Szabo. This, again, has suggested that his real name might not even be Nick Szabo, as it just might be his pen name. There is very little known of Nick as there is no verifiable age, education, location, or even former work profession; therefore, within the technology world, he has become the number one candidate for the birth father of Bitcoin. Apparently, anytime he has been asked if he had anything to do with Bitcoin, he has always denied it, and for a while now, once again, he has gone silent. Unfortunately, when it comes to the media, there is so much fake made up news that it's just unbelievable. At the beginning of the 21st century, the internet was the only

actual source of news; however now that most newspapers have moved online, it takes an enormous amount of time to research the true. That's being said, most of those who were always trying to find the truth, indeed, don't read newspapers and fake news channels, and I am talking about IT Professionals that only study about technology. Even though when a technological invention, such as Blockchain, comes into the news, nerds become obsessed to find out who exactly is such a great designer, and they begin to do their research until finding the truth. So far as it seems, most tech gurus are pointing to Nick Szabo as a real creator of Bitcoin. When it comes to possible candidates of the father of Blockchain technology, there are many assumptions. It all depends on who you ask; however, I wanted to introduce some of the main characters who might have some involvement in Bitcoin creation. Many people believe that Blockchain, due to its complexity, might have involved many characters, instead of only one certain individual. When Craig has been asked, he said that he had help. However, he was the main person behind it all. Therefore, many have begun to believe not Craig, but that Satoshi Nakamoto could be representing a group of individuals instead of man's name. In Japanese, Satoshi means clear thinking or wise, Naka means inside, and Moto says Foundation. These three words can be put together in many ways. Nevertheless, one of the most common would be that he, or the team, is announcing something like: I am wise, and I fully understand this system from inside out. You may replace the "I" with we. Still, Blockchain was certainly not a product of a mistake. The creation of this technology indeed required clear thinking and must be able to understand fully every single detail of it, and lastly, Blockchain is a large foundation. The opposite thinkers are confident to say that due to the Blockchain's structure, the idea must have been born in a single mind. Therefore, having a team thinking together, creating something similar, would not be as detailed as it is. I am talking about people that are not average techies, but software developers, and were part of building the internet since the early ages. Again, Nick Szabo comes to mind, instead of an Australian business magnet, neither an old Japanese man who was not involved in anything for an extended period. I will now close this chapter, and let your imagination decide who Satoshi Nakamoto is. Still, as I mentioned before, it may all depend on the date of reading this book; but for now, over a decade after the Invention of Blockchain technology, we still have no evidence to prove 100% who Satoshi is.

Chapter 6 The Distributed Ledger System

I would like you to think of the ledger system as a family tree; but, instead of people's names, the huge ledger system holds information about payment value and addresses. In regards to the amount values, the ledger holds all the records of payments back to the first transaction that was ever made. In regard to the addresses, there are no URL's or location addresses. Instead, these are Bitcoin, or any other cryptocurrency addresses. The ledger holds a series of transactions of all cryptocurrencies. Additionally, the current values are continually computed of the previous transfers. One part of the ledger is representing the value that has been assigned, some other parts of the ledger represent the date and time of each transaction. This is very similar to any of the current Banking systems. You can see who transferred to what account, what date and time, as well how much was each transaction; however, the ledger has no banker. Also, the addresses are not representing names of the individuals, neither who holds what amount; therefore, you can call this an anonymous ledger system. What you have to understand is that when it comes to an individual's bank account who has no relatives, the bank could seize that account. In addition to banks, even the Police, FBI, or any government official can take any bank account if they find a possible reason for it. When it comes to a Bitcoin account within the great ledger, the only person who can access it is the person who has the password to that account. Of course, it's dangerous; if you accidentally lose the password to your Bitcoin wallet that the ledger holds, whatever value it has will be lost forever. With your bank account, if you lose your password, you call the bank, they ask security questions, and once you prove that you are the owner of that account, the bank will provide you access. On the other hand, having a Bitcoin account, no bank will be able to help you to access your account. The ledger is visible to anyone, as it's completely de-centralized. Therefore, everyone can see your Bitcoin account, as well how much value that wallet has. However, no one can tell that account is connected to you. To view real time Bitcoin transaction, visit the following website:

https://www.blockchain.com/btc/unconfirmed-transactions

Once you are there, you can pick any address from the live transaction, and then click on the "hash" value, which is normally a very long address. This will take you to the "Summary" page. Then within the summary, you will see

the date and who sent to whom what amount of value in both Bicoin and Dollar, and you will also see the fee the network has taken for that particular transaction. Next, if you click on any of those addresses, wither who sent the Bitcoins and whoever received it, it will take you to the “Address” page where you can see all previously made transaction as well the Total amount ever received and the total amount ever sent from that particular address.

Due to the Blockchain technology, every transaction is confirmed for its validity and goes into a block; then each block will join to the previously validated blocks, then eventually they all will form a chain of blocks, that we call Blockchain. Every Bitcoin citizen is required to keep a copy of the Blockchain, after each block that gets created by the system, every Blockchain member receives a finalized sealed block. Then the system checks each block automatically and adds each block to each citizen. This is how Blockchain holds every transaction and every value that was ever created. These methods ensure the legitimacy and correction of every transaction without any central authority. If all that sounds unfamiliar to you, just understand that is completely automated by the system, and you, as a Bitcoin citizen, do not need to do any calculation, and it would probably take a very long time anyways. Each transaction, once validated, is sealed into the ledger; this process is carried out by the miners. When a new validated block arrives, each new block must be added to every citizen’s Blockchain; however, before accepting the new block, everyone checks the logical continuation of all the values in the new block, to make sure that all the transfers of costs are legitimate. This also prevents any replication of transfers or any counterfeiting done by hackers, or people with bad intentions, trying to steal Bitcoin or any other cryptocurrency. This is a crucial step, as this validation will remain within the great ledger and within the Blockchain forever. This process uses hashes for competition, to validate each block, and make sure that each citizen receives the same record. Hopefully, I didn’t confuse you by adding some extra bits on how the ledger becomes distributed and what process it uses for the purpose of validating each transaction. The reality is, that technically multiple protocols are working together to achieve each validation process. Also, you have to understand that thousands of the operations are made in each of every second. Consequently, I have avoided the technicality as much as I possibly could. Also, if you are interested viewing real life blocks being created, you can visit the following website: https://www.blockchain.com/btc/blocks?page=1

Once there, you can see the “height” of each block, the “hash” of each block, when that block was mined, “Miner” which is the mining pool and the size of each block. Out of curiosity, you can check this page out and click on each miner or hash of the block, but you might be thinking who are the miners in the first place right? Well, we will discuss the miners within the next few chapters.

Chapter 7 Who are the Bitcoin Miners

Let's first think about how new value enters the system. Back in 2008, Satoshi Nakamoto only created 50,000 Bitcoins to start the process. If you think about it, had he built all 21 million in the first place, the Bitcoin would be worthless, and the idea would have been dumb. Instead, Satoshi started with a moderate amount of Bitcoin creation. Yet, as the Bitcoin community grows, more and more value would be required for the system to be kept alive. There is a particular process that is needed for the system to be maintained; Satoshi has come up with the solution by creating a role. This solution is not only solving one, but two issues; permanently validating transactions and adding new value into the existing system. The role is called "miner". Miners can be individuals, or any Bitcoin citizen. However, over time, many large companies have been formed, such as Genesis Mining, AntPool, SlushPool, F2Pool, where you, as an individual, can join and rent their mining facilities. There are many other miners who over the years have created a pool, and many of them also offer to join these pools for certain reasons that I will discuss shortly.

NOTE: If you want to look at all miner pools exist currently, you can visit the following page: https://www.blockchain.com/pools

Here, you will see all pools, but you might see a large percentage of them or "Unknown". This is not the company name of course but those miners are mining solving blocks or mining Bitcoins using TOR browser. Basically they don't want to share with anyone who they are and where they are.

First, let me explain why they are called miners and what it is they do. They are called miners as the analogy has been used with gold or any other precious metal. They work together to create new value, similar to gold miners who are digging underground. However, Bitcoin miners are sealing each transaction into the ledger. Therefore, we could call miners, finalizers or authenticators. To get rewarded for such work, the miners receive Bitcoins, and this is how new value is added to the system. The miners validate, authenticate, certify, and finalize the transactions by specific processes. Once the miners have created a new block that is accepted by the citizens, the record of the transaction cannot be modified, making it a permanent information. This will also become irreversible. Therefore, no one can ever

challenge it or change it in the future. The miners are sealing the blocks, which in itself can take an enormous amount of computing power, assuring that they cannot be easily replicated. There are multiple methods that each miner may use for the validating processes. Some of the miners may use different software, even creating their own in-house made software to speed up the authentication process. However, it doesn’t matter what software they use, as all of their work will be checked. It starts when a miner begins to gather transactions that have been broadcasted on the network, and then starts checking those transactions, and eventually sealing those collections of transfers and operations into a new block. A miner receives Bitcoins as a reward for each sealed block that is added to the Blockchain.

Chapter 8 How Bitcoins are created

Explaining each block creation can be done in multiple ways and many sounds very confusing but it also depends on your understanding of the technology. Therefore, hearing or reading it the first time can be difficult to comprehend. I already explained that miners have an unusual role for validating each transaction in the form of a block. Now, let's discuss what it takes to create each block.

1. Start a new block. Even if the miners are half-way done validating a block, eventually, they will drop everything and concentrate on starting a new block.

2. Select a new transaction. This is when the miners are choosing from thousands of operations that are broadcasted over the network.

3. Check priority of the transaction. This time the miners can go back to number one by starting a new block if they find that the transaction they have selected previously is not that significant. However, if the priority is high, the miners may go on and move to the next step.

4. Check that the transaction is valid. This is a process that every miner must check, there is no exception of avoiding this step for any miner. However, if the transaction is found to be faked, or not valid, the miners have to stop the process, and go back to number 1 and start a new block and get another, hopefully, valid transaction.

5. Accept the transaction. If the previous transaction was tested as a valid transaction, it must be accepted.

6. Seal the transaction. Again, if the transaction has been found valid and accepted, now it's time to seal that transaction.
7. Add the transaction to the transaction tree inside the block. This process can only be done once all previous steps have been

verified.

8. Check for the size of transactions. The miners need to check if there are enough transactions within the transaction tree to seal the block. If there are not enough transactions yet, the miner will not be able to seal the block until there are enough transactions. Therefore, the miners must go back to number 2 of selecting a new transaction again, and again, until there are sufficient transactions for sealing the block.

9. Check interruptions. This is the process where the miner must make sure that no other miners have sealed the block in the meantime with the same transactions inside the block.

10. Seal the block. Once there are enough transactions for sealing the block, the miners will seal the block.

11. Broadcast the block. The miners must broadcast the new block that has been sealed; however, if the miners have been interrupted within the block sealing process, they might have to start a new block all over again.

12. Start a new block. This is the next step in the process; however, as you see, we are now back to step number 1. As I mentioned before, miners might get interrupted while they are sealing the block and once they broadcast it, if another block has already been sealed by another miner with the same transactions within a block, the block will not be accepted. Therefore, they must start a new block.

Each block is created about every 10 minutes. As a result, 144 blocks are created each day. The miners who have successfully added a new block into a Blockchain get rewarded a degree of Bitcoin. The reward for each new block creation used to be 50 Bitcoins from 2008 until 2012. The reward for a new block gets halved every four years; therefore, from 2012, until 2016, the award for each new block used to be 25 Bitcoins. Until 2020, the reward to a miner for a new block that is added to the Blockchain was 12.5 Bitcoins; but

since 2020, it is only 6.25 Bitcoins until 2024. From 2024, the reward will drop to 3.125 Bitcoins until 2028 and so one. This process will continue until 2140 until the last Bitcoin will be created.

Chapter 9 How secured is the Blockchain

You might think, “OK, fine, Blockchain is a high technology that will positively change the world.” But, the question remains, “Is it secured?” The short answer is yes. But first, let’s think about what the system has currently achieved. The reality is that anything can be hacked and compromised that is connected to the Internet, or connected to a system that has the connection to the web. Many devices do not use any connection and still can be broken into once you have physical access to it. Such might be a laptop or desktop computer that can be broken into using a Linux cd, and booted using that. If you want to go further, let’s take a look at banks for example. They are getting compromised all the time; of course, they have stopped announcing these types of incidents, as they would have no customers left if they would carry on doing so. The director of the FBI was hacked by a teenager in the end of 2015, and most people think it’s funny. Still, when you think about the security within the FBI, it is very well organized, yet still hackable. The FBI might not be the best example to mention, as even Kevin Mitnick hacked the FBI for three long years, and listened to the agents’ phone conversations while Agents were talking about Kevin. Anytime they talked about Kevin as they found out where he stayed and they will raid his place, Kevin knew about it, so if just moved to another place. When you look at the NSA, aka The National Security Agency, you probably have heard of Edward Snowden already, who walked out with documents that are considered to be secret; that still shows that even the NSA has weaknesses. Confidential or even secrets can be leaked. All those expensive Firewalls, Intrusion Prevention Systems, or Intrusion Detection Systems are worthless if they are not upgraded correctly. Also, you have to understand that having all that security does not mean anything if someone has a social engineering skill set and figures out the password to any of those devices. The result would be dramatic, and they always are, but most of the great financial institutions have stopped talking to news channels about being compromised by hackers as it would only damage their image, and it would become an embarrassment. Because companies keep all their data centralized, hackers only have to go after a specific organization to compromise its systems; that is why hackers know for a fact that anything can be broken into. To hack into any system, it’s only a matter of time and proper planning; however, when it comes to a system like

Blockchain, it is highly unlikely. Although experts say that it is not impossible, it still would require an enormous amount of computing power. Blockchain has no firewalls or any Detection or Prevention system that would protect it. Instead, Blockchain's power comes from the fact that it is completely decentralized. What I mean by that is simple really. Though, I will do my best to explain it in everyday English. Because Blockchain is an open source technology, anyone can run the software. You may choose not to ever buy Bitcoins, or invest in any cryptocurrency. Nevertheless, you might become part of the Blockchain community by running a software called Blockchain. The software itself is free to download and use, and you will have no obligation to anyone whatsoever, but once you decide to run it, you simply become part of the Blockchain community. Once you become such member, your device will become part of the Blockchain and each time a new block is created your device will also get a copy of that transaction. As your device has now became part of the Blockchain, this is another device that should be hacked to compromise the block chain thoroughly. Because your device is now running a Blockchain software, it's now also contributing to the existing decentralized system. There are no centralized copies and every user is trusted in the same way as the rest of them. What I mean is that no master node exists, as every single device has the same replicated information, making it nearly impossible to hack. The Blockchain is running for almost a decade, and it has never been compromised, not once. It is fascinating, as the Blockchain has a bounty of 7 Billion dollars to anyone who can compromise the system, offered anonymously. Due to the price on Blockchain's head, it has become the primary target for many black hat hackers, as well as large criminal organizations, and Cybergangs, for years. Still, Blockchain has not been hacked yet, not even a slowdown of any kind has ever happened. This shows that the core functions have been structured very well; but, as I mentioned before, anything can be hacked, as it's only a matter of time. IT professionals always believe that with technology expanding rapidly, in the future, anything is possible. Quantum technology defines the way how the Blockchain system can be hacked. Nevertheless, it would require hacking the million-plus machines currently running the Blockchain software. Additionally, to actually hack all those devices, it would need to be implemented extremely quickly to be successful. Speculations about Satoshi himself are still in a shadow; moreover, as we don't know who he is and what he is capable of, one thing is for sure: he

designed the system. Therefore, he would have access to the very first block that he created, and he would be able to manipulate the Blockchain system if he wanted to. As time has passed, multiple Blockchain technologies now exist, and Bitcoin, itself, has grown its value; people have also begun to invest large amounts into various cryptocurrencies. Over the years, people have lost interest in who Satoshi Nakamoto really is, or he, just simply, has been forgotten; however, if he or she is alive and decides to manipulate the system, it could be possible, and I’m sure that the outcome would favor most.

Chapter 10 Comprehending Business purposes

In technology, there are many geeks, myself included. Though, some people differ from one another. How can I define a geek to you? Well, there are many different kinds out there, so let me begin with friendly geeks at first. Video games have changed the world, and many youth, or even adults, have become obsessed with their favorite games. For those who have never played online games straight through a whole night or day, or both, for days—might find it difficult to understand why certain people become addicted to video games. Those who just love to play and spend money on games is one thing, but there are other types of geeks too. Some nerds are obsessed with new tools and software and believe they MUST be tried out ASAP, even if some of this software is downloaded from torrent websites illegally. There are other geeks too, who would not necessarily download everything for free, but instead would purchase the original software or tools to feel better by having the real thing. The authentic software always provides a better feeling, as well, many geeks buy it out of respect for the creators, contributing to the software developers and designers. When it comes to Blockchain, there are multiple companies that have been formed recently which are designing a particular protocol that would allow certain online games to be played by using their own in-house built cryptocurrency. Topping it off, they have created excellent online games that once the gamers join and play, they would participate in their cryptocurrency by providing CPU or GPU power from their Game PC-s, PlayStations, X-Box-s and so on. Because these protocols would be fully utilized and continuously contributed, its value would begin to increase dramatically. As you can see, Blockchain would allow creating not only a new cryptocurrency, but an online gaming community, who would use a particular Blockchain technology. I have mentioned an example of gaming. On the other hand, there are many companies that are now into similar Blockchain technology, such as music on demand, movies on demand, social networking sites and so on. One of the biggest inventions so far, using the Blockchain is the creation of smart contracts, such as Ethereum. There are many other alternative Blockchains that exists to date, and each will shape our future at some point. To mention some other important choices, there are various decentralized crowdfunding, healthcare, supply chain, blogging sites, and real-time sharing; but the biggest

of all is IoT. IoT, also knows as Internet of Things, for Blockchain is increasing rapidly in recent years. Internet of Things is also called smart devices, or connected devices, that are physical devices, or even driverless vehicles. The purpose of these devices is to log in to the network and begin to share data one to another. Automating everyday life is a small-scale business, such as software, electronics, and sensors that would interconnect to each other. Nevertheless, when it comes to large scale, that's where the bit money is, such as virtual power plants, smart homes, intelligent transportations, or even smart cities capable of operating using Blockchain technology. There are big scale business plans for big boys that require years of planning; however, the technology to allow it, now exists. These projects would provide opportunities for direct integration of the physical world into computer-based systems, resulting in improved efficiency, accuracy and economic benefit in addition to reducing human intervention. M2M – Machine to machine communications already exist. But, Blockchain will enhance this beyond, by speeding up virtualizations and trust collecting data into blocks, helping to use our data more efficiently. Currently, there are thousands of banks all over the world. Therefore, the current banking system will not stop tomorrow. It will require having at least a decade, if not two. But, the technology already exists to use other methods than banks, all that is needed is for Blockchain technology to be applied by all our business partners, or employees, or employers. It is straightforward really. Yet, most of us are very comfortable with the current system; therefore, the change might take a long time. When gold was retired as a currency and paper money was applied, it took many long years to implement and make everyone understand that wages are now not paid in gold, but with paper. As I mentioned before, gold is still an excellent payment method in most countries; but, it is not accepted everywhere. When you go to the local supermarket, you cannot pay by gold, well some places are possible; nevertheless, most places will not accept it. Same as when you purchase something online, you cannot pay in gold, and there are other reasons too because it is an old method. First, let's look at the flexibility of the gold. Imagine that you want to go to the local Coffee shop to have a cappuccino. The idea to pay in gold for a cappuccino is daunting. How would you break or cut the right amount of gold to the shop owner, besides the point, what if you make a larger cut than you have intended in the first place? The point is that any precious metal as a payment method cannot be widely implemented.

It’s heavy; it’s difficult to cut or break to the right amount of pieces required; therefore, the idea of using it in the future for money is just not suitable. Unfortunately, paper money or cash, keeps on getting printed all the time. Therefore, it’s impossible to tell how much is on the market. The more and more it’s printed, the less it’s worth. From history, we have learned that after a while there is so much cash getting printed that eventually, it all becomes worthless. Inflation becomes the main issue, lots of people become poor with all their saved money in the bank, and then governments begin to print new paper money for the so-called new economy. The problem is that this system has failed miserably—on multiple occasions; as a result, we all know that it’s worthless. The problem is that this system is centralized by governments and banks that average people have no power to go against. Digital currency on the other hand is unstoppable, and such like Bitcoin, can change the current system very quickly. Another issue with paper money is that it is very easily counterfeited. There are countless incidents every day involving all kinds of paper money. It doesn’t matter how well paper money is made; it can be duplicated. Consequently, counterfeiting will always be around. Cryptocurrency on the other hand cannot be faked, cannot be copied, cannot be counterfeited. Because Blockchain represents trust and the exact amount of digital money, keeping just that in mind, you have to understand that cryptocurrencies easily can overtake any paper money, especially if it’s centralized. Only 21 million Bitcoins will ever be created. So how can there be enough for everyone? Well, each Bitcoin has 100 million Satoshis. I am not very good at math, so I have used a calculator to understand how much Satoshi will ever be produced, and the number looks like this: 2,100,000,000,000,000. There are close to 8 billion people living on earth. So next, I have divided the huge number by 8 billion, to understand how many Satoshis each person on earth could have distributed equally. The number I got is: 262,500. The reality is that currently, 60% of the population will never even have $20,000.00 saved in their whole lives; But, before you think that is the final outcome; let me tell you something else. Blockchain technology allows each Satoshi to be broken into other fractions such as another 100 million pieces, and if that’s still not enough, those fractions can be further divided into another 100 million of even smaller portions, and so on, and so on. That being said, I hope that you understand that Bitcoin itself, can supply the whole world when it comes to a new currency. But, there are many other currencies already, and the banks have begun to think about

creating their own digital currencies too. Currently using swift, making international transactions can be a pain. Instead of taking a few seconds like Bitcoin and other cryptocurrencies, it can take 3-5 working days. Besides taking too long to transfer money, it might also be unavailable to individual countries, not to mention the fees. Making payments with several cryptocurrencies that are using the Blockchain as their platform, are not only super-fast, but have very cheap costs, if any. Additionally, anyone can have a Bitcoin wallet online. When you go to the bank to open a new bank account, you must fit all the criteria that the banks ask for. Such might be, that you must have a valid address, you must be 18 years old, you must have proof from your employer that states your occupation as well your wages and so on. Instead of all these headaches, if you have a smartphone, you are able to open a Bitcoin account without any of the aforementioned criteria. Then, in a few seconds, you can begin to even make international transactions. The current issue is that if I want to buy something from you, I have to make a transfer from my bank through PayPal, to your bank, which eventually would pay you. It takes at least one other so called trusted 3rd party to make a payment. But, Blockchain would validate that transaction for us. Therefore, we wouldn't require banks or any other trusted 3rd parties anymore. All that is necessary is internet access for few minutes. You have to understand that there are 1.7 billion people currently have no bank account, for various reasons. They might not be qualified enough; they might not even have the proper clothes to enter a bank. They might just choose not to have a bank account, but mostly, so many people just live too far from any bank. Therefore, they have decided not to have one. They might have internet access here and there, so Blockchain might as well become their bank, right? Why not? It would be very beneficial to them, and it's already happening with lots of people. What the banks have realized is that it might be a good idea to create their own cryptocurrency, so in case Blockchain takes over the world, at least they are prepared for the big boom.

Chapter 11 Introduction to Blockchain Attributes

Blockchain is a new technology but once you take a closer look at it, you will realize that the ingredients are pre-existing, and all that was needed was to stack them together. Some inventors do get offended once a new and better idea takes over their own, especially if it's even cheaper, faster, or often free of charge; but this is part of the innovation that we have always experienced. When it comes to technology and you invent something today, it's almost guaranteed that once it's on the market, there are a significant amount of people already trying to copy or make it better—whatever that service or software is. Therefore, innovation is inevitable. It is just as true when you look at physical storage for keeping data, such as music, video, or software. What happened over the years is this: the less space required the greater the quality became; in fact, most data, movie, and music, are now streamed from multiple sources; therefore, the idea that money will be streamed one day should not be surprising. I still remember when I used to buy VHS and DVDs, also cassettes and CDs. Also, remember when there were no mobile phones? Then, once they reached the market, I was able to make phone calls, and send text messages pretty much from anywhere, or even play the game called snake. After the introduction of the internet, I was always waiting to get home so I could access the network or I had to call someone to check weather forecast or other useful information for me when I needed it. Though, less than two decades later, I can now store hundreds of movies and music albums to my cell phone, as well capable of Skype, video calls, and access any internet page from anywhere in the world. As you see, no one can predict what happens with technology over time. Blockchain is where the internet was back in the middle 90's. The internet seemed a nerdy idea, and most people thought that it was all about email. Like nowadays, some people believe that Blockchain is all about Bitcoin. The reality is that e-mails might have been slow and people weren't interested in them; still, in few years, most companies have moved online and of course become even more successful by doing so and the main tool to use for both internal and external communication within the infrastructure is e-mail. Back to Blockchain innovation and its ingredients, let's take a look at them and understand a little bit more about them.

Chapter 12 Peer-to-peer network

To keep the Blockchain running, it requires a network that resides on the internet. Furthermore, within the network, there are certain exchanges, for purposes of updates. These updates are required to continuously keep the distributed ledger system up to date with the latest block. If you turn your computer on and start to run Blockchain protocol on it, it will become part of the Blockchain network. Next, I would do the same with my computer, then my machine would become part of the network too. Every single device that is connected to the internet, and running Blockchain, becomes part of the network. This way all those devices can communicate with each other using the internet, and keep on updating each other. Because there is no master node or a centralized machine that has a different purpose than the rest of them, this network is called peer-to-peer network. Peer to peer networks have existed for a long time. Therefore, there is nothing new about it. However, because it has no master node of any kind, this is not a centralized network, but a decentralized P2P network. This is very important, as it tells you that there is no boss of any kind; so, it decreases the possibility that one or more nodes on the network might be able to manipulate the rest of the nodes. Manipulation of any kind is simply impossibly, and that, in itself, is proof we can trust the system. The network itself is solely based on a technology that's existed previously; however, this time it has a different purpose. What you have to understand is that when it comes to a peer-to-peer network, there is no central server or central client. In traditional centralized networks, there is the primary server, or central servers, and multiple clients; and the way they are connected is that the servers are always dictating what the clients can have. Peer-to-peer networks, on the other hand, are completely different, as all nodes on the network serve both purposes, they are all servers as well as clients. Meaning, no one machine can have a bigger decision power than any other on the same network. Therefore, P2P networks are always working together, making decisions together, and equally distributing those to all nodes on the network. Another problem with centralized networks is that if one node is ready to share the latest news with the rest of the network, first it would have to send the traffic to the master node or server, which then would be able to do many things. The server could manipulate the traffic before forwarding to any other node. Managing the traffic would be easy on the server node, as once the server would receive the traffic from client A, the server would not send the same traffic back to client A (as that was the source in the first place). Instead, the server would send the traffic to the rest of the

clients, but if this trade would be manipulated already, neither the remainder of the nodes or client A would never find out about it. Another issue would also be if the server would decide to send the traffic only for a particular group of clients, instead of all of them. Again, this could reduce the power of an extensive peer-to-peer network, and in the case of the Blockchain, this would not be an advantage. The worse that could happen in a centralized network is this: once the server would receive traffic for the sake of conversation, data about the latest confirmed block, imagine that the server would decide not to share this data with any other client. This would just put the Blockchain out of business. Therefore, the only way that the system would operate is to use a decentralized P2P network. In case you wonder how the server would make such a decision itself, well, it would not. Even though administering a server, or a small group of servers, may be straightforward for a person; when it comes to a P2P network, a person with evil intentions, like hacking purposes, or traffic manipulations, would have a hard time to do so and the reason is straightforward. Administering a large group of machines manually that reside all over the internet is nearly impossible. This is the reason why if you want to open a company, and you want to be the boss, you would create a traditional centralized network by having a master node that you can administer anytime you want. Again, P2P networks have no boss. Therefore, there is no one to blame, and every machine on the network shares the same responsibility. In any system, centralized or not, there is always some delay. This is called latency. By the time one device reaches the other, it’s just never the same amount of time. Technically, latency is the time defined while the data travels between its source and final destination. This is something that you may consider understanding as data propagation can take some time, especially when there are thousands of nodes on a decentralized system. Let’s look at an example for better understanding. Imagine that node A is ready to share its latest block with node B, C, and D. P2P networks are also known as dumb networks, as they have no idea what kind of data they are transferring; all they know is once there is data that needs to get transferred across the network they will do a broadcast making sure that all nodes are receiving the same data. So back to our example of four nodes and their data propagation. Imagine that node A is located in Los Angeles, US; node B is located in Sydney, Australia; node C is in Cape Town, South Africa; and node D is in London, UK. They will all receive the same data; however, some of the nodes may get the data earlier than the other nodes.

Therefore, the order of the transactions might differ on the nodes. In summary, peer-to-peer networks are helpful for the following reasons:

- Reducing overhead by not sharing data over multiple nodes instead of keeping everything in one centralized location.
- Reducing risk of counterfeiting and manipulating data.
- Reducing third party interference, therefore, each transaction of smart contracts have fewer fees as well faster implementation.

Chapter 13 Understanding Hashing

This is another topic that most people just skip if possible, and I can't blame them. Cryptography has complexity that not exactly everyone dreams to learn about. There are many different kinds of cryptography that exist; however, I will try to do my best to keep it simple for you to understand. There is classic cryptography that has been used since the ancient times by the Greeks and Romans, even in Egypt; however, our focus is modern cryptography, especially the one that is related to computers. Before I drag you into it any deeper, let me elaborate some basic terms that are vital to understand before diving into Cryptography. Hashing is referred to a fixed sized string of numbers, for example, 128, 256, 512, 1024, 2048 numbers. Hashing can be performed on various files, such as text, images, audio files, video files, or even software. It produces a unique hash based on that the particular file. An individual file goes through a hash on one end; then comes out scrambled on the other end. It doesn't matter what kind of file you try it out on; the result is always different. For example, you might try to put an md5 hash in the word "Blockchain." The hash would be completely different than the word "Blockchain1."

Note: MD stands for Message Digest, and the number 5 is its version number. Basically, MD5 has taken over MD4 hashing. Let me explain how much of a difference there is between two very similar words. As I mentioned the word "Blockchain," I will perform and generate an md5 hash on it. Ok, so the md5 hash value for "Blockchain" is:

5510a843bc1b7acb9507a5f71de51b98

However, now I will perform the same md5 hashing on the word, "Blockchain1." Let's see the result:

1150228f14788047028d774b7c83c5a6

As you see, this is a completely different outcome; this is because the word is different, although very similar, it is still a different md5 hashing value. Let's try to do this now with a number, and for simplicity, I will use very few figures so you will see how powerful hashing can be. This time I will perform md5 hashing on a number string of 123, and then 124, and see if there is any difference. Let's begin, shall we? Ok, so I have performed md5 hashing on

the number string: 123, and the hashing value is this:

202cb962ac59075b964b07152d234b70

Now I will do the same md5 hashing on the number string 124, and the hashing value is this:

c8ffe9a587b126f152ed3d89a146b445

As you see, again, it's an entirely different outcome; therefore, hashing itself can provide excellent security. However, I will move on to more in-depth. In case you think I am some genius, or just making up the md5 values, I would suggest you visit the link for md5hashgenerator and practice for yourself. Perhaps you can start with the same words and number strings I made examples of. The website to visit is: http://www.md5hashgenerator.com/

MD5 is also case sensitive; therefore, using the very same letters, changing only one character to uppercase, the result of MD5 value would also be completely different. The closest example I can give you is fingerprints or DNS. Those are also unique, and there are no two people who have the same DNS or the same fingerprint. Hashing has been widely implemented, mainly used by software developers. One of the main reasons is making sure that the software is not modified or corrupted while downloading it. Personally, I had an issue before when I upgraded a Juniper Switch with a new code, which has gone into Rommon mode because I was too lazy to check the md5 hash value of the software. Luckily, I was doing it within a test environment, and not in production network; however, it caused great pain and lost hours to recover the switch to its previous configuration. In my case I downloaded the code from the right source; but, it seemed to be that our Proxy server must have corrupted halfway. Still, if I would have checked the md5 hashing value of the new code, I would have been more successful at the task. MD5 hashing is excellent; however, it is not called cryptography nor encoding. MD5 was implemented first in 1992, and if you think it's a little old, then you are right. MD5 has been compromised several times due to its vulnerabilities, alone it is not sufficient to provide the best security. That being said, let's move on to what Cryptography is.

Chapter 14 Cryptography Basics

Cryptography is a process defined by data being converted into a certain form

so that it is only available to those for whom it was originally intended. However, converted data is inaccessible to an unauthorized end user.

Encryption: What the process of encryption does is simple. It transforms a particular data into a form that is unreadable. The encrypted data has another common name: Cipher text.

Decryption: The process of decryption is responsible for converting the unreadable data back into its original form so that it can become readable again. For example, a simple decrypted text, after decryption would become a plain text. Once data has been encrypted, and it has been sent to the destination of the recipient, there are different ways that can be used for data decryption. There are two prevalent techniques to encrypt and decrypt data, one is using Symmetric keys, and the other is using Asymmetric Keys.

Symmetric Key: Using symmetric keys is easy. When encrypting, as well decrypting, we only use the same keys. An example here would be a door. When you go out to the store, you lock your door using your key, and once you return from the store, you would use the same key to unlock your door right? Well maybe I am wrong; however, typically the same key is used for those purposes. The symmetric key algorithm is very fast, in fact, thousand times faster than using asymmetric keys. When we were talking about symmetric keys, same keys, they are also called shared secrets. As you can see the problem here is that both the sender as well the receiver must use the same key for both encryption and decryption too. Of course, this is not an advantage when it comes to security, and the Blockchain is certainly not using Symmetric key algorithms. I wanted to introduce some of the basics before we dive into more depth, such as asymmetric key algorithms.

Asymmetric Keys: Blockchain uses Asymmetric key algorithms as part of other algorithms it uses. Therefore, this topic is what you might have been waiting for. To implement Asymmetric key algorithm, it requires having two different keys. One of them is called “Public” and the other is called “Private” key. The reason for having two keys is simple. One of the keys will be responsible for encrypting information to become a cypher text, and the other is to decrypt the information to become plain text. The private key would be generated by the originator, the one who would encrypt the

information, and this private key must be kept secret at all times. However, the public key would be available to anyone, this is why it’s called the public key. The asymmetric key algorithm is much slower than a symmetric key algorithm; however, the security is more complex. Therefore, it is harder to be hacked. Both, public and private keys are mathematically interconnected one to another, meaning that each public key has only one corresponding private key. There are few algorithms like that. However, Blockchain is correctly using the one called: Elliptic Curve Digital Signature Algorithm. This situation is a little different for how Symmetric key algorithm works. Once the private key has been used to encrypt the information to become a cypher text, it is necessary to use the public key to decrypt the information back to plain text. On the other hand, this process can be interchanged and used the opposite way too. For example, I would encrypt the information using the public key; then I would decrypt the scrambled text back to plain text using the private key.

Chapter 15 What is a Digital Signature

When it comes to a legal contract, the traditional way to do business is that both parties, the buyer as well the seller, has to sign the contract, amongst many other documents for legalization. This traditional way of signing contracts is carried out with handwriting using a pen. However, there are other ways to authenticate certain documents, and one of the most known is using digital signatures. Digital signatures are very similar to standard traditional handwriting signatures. However, they are much more secure. When it comes to handwriting signatures, there is a long history of them easily being faked by a pro or anyone with a little practice. Digital signatures have overcome the issues of counterfeit signatures by using some simple methods. The digital signature provides the recipient unique information; therefore, it provides authenticity.

- Integrity: This is for making sure that while the message was in transit, it had no alteration or any modification.
- Authentication: This is to provide the authenticity of the sender.
- Non-repudiation: This is, so the sender cannot deny that the message was ever sent.

If you're wondering how the digital signature is created, as well verified, let me begin by explaining it. Imagine that you want to create a document by adding a digital signature to it so that anyone would know that it belongs to you. What you can do first, is to hash the data. Next, you can use a private key to encrypt your data. That's it, as the encrypted hash is your digital signature. Taking this further to prove that it is indeed your digital signature, you have to send the document to someone who can then decrypt your data. Once you send your text to your friend, you also have to carry the digital signature along with the document. Once your friend has received the document, he or she should decrypt your document by using your public key. This time the result of the hash value of the document would be HASH1. So, if your friend applied the same hash algorithm on the received document, the result of the hash value on the received information would be HASH2. Next, your friend should compare both hashes: HASH1, and HASH2 and if the values are the same, it would be proof that your document had no alteration in transit, the document is originated from you, and it is indeed yours.

Today’s digital world demands more flexible and responsive solution, then handwritten signatures. Instead of wasting time by using traditional signatures, digitally, you can handle contracts in a matter of minutes. Using digital signatures—deals can be closed in minutes—not weeks. Lots of software literally lets you create digital signatures in seconds. All you have to do is select a document on your computer, right click, then choose using digitally, set your password on it and send it off by e-mail. The process is completely paperless, and the digital signature just as valid as the one made without ink. Furthermore, not only using a computer but a new way of using mobile apps, by having a mobile ID, you can sign documents, make bank transfers using your cell phone only. This also means that you can be anywhere in the world, and in seconds you can authorize bank transactions as well signing any documents. Actually, research has shown that using digital signatures helps an average person save one whole week of free time in every year. You may use this time as a vacation. However, there are other benefits too. Paper. We can save tons of paper around the globe using digital signatures.

Chapter 16 Comprehending Logarithms

Let me ask you what do you think the difference is between the number:

0.0000000159, and the number: 0.00000000159?

Well, if you feel pain in your head already don't worry, it's completely normal. Logarithms are helping us deal with small numbers; though, in some cases, huge numbers. This leads to the concept of logarithms. What logarithms are fundamentally about is to figure out what power you have to raise to, to get another number. Logarithms are yet another component of Blockchain technology that is going back in history to the 17th Century. This discovery has provided a new function that has extended beyond the scope of algebraic methods. Logarithms were publicly announced in 1614, and it began to simplify difficult calculations that contributed to the advance of science, as well, surveying and celestial navigations. Back then they had created different logarithm tables for various calculations; however, nowadays in computer science, logarithms still exist. Let's begin with a simple example for better understanding how logarithms actually work.

To have two to the power of three that means two times two times two.

23 = 2 x 2 x 2 = 8

In this example, we have three numbers to work with.

2 > this is our base number

3 > this is called the exponent, that will determine the number of times that the base number should be multiplied.

8 > this number is known as the product.

Now imagine that the exponent x is unknown, in this case 2x = 8 so we want to find out how much is the x, well we already know that, because of the above example; however, sometimes it can be lot's more complicated than this simple example. If you are only interested in the exponent, the mathematical notation: x = log2 (8)

The pronunciation for the above mentioned is: x = log base 2 of 8

Exponentials x = 23 and logarithms x = log2 (8) are each other's opposites

The goal of exponentials is to calculate the product: x = 23

The purpose of logarithm is to calculate the exponent: x = log2 (8) = (8 = 2x)

So, we needed a numerical procedure that is easy in one direction, but hard in the other direction. When the generator has raised two different components, the solution distributes uniformly around the clock. If we raise any base number to any exponent x then the solution is equally likely to be any number between zero to 17. However, the reverse procedure is hard. For example, having the product number and you want to find the exponent is hard to do. This is called the discrete logarithm problem. Now we have our one-way function, that is easy to perform, but hard to reverse. It is trial and error really, but if you want to know how hard it can be, then let me tell you. Well, having small numbers, this is easy to reverse engineer; but, if we use a prime modulus that is hundreds of digits long, it becomes impractical to solve. Even if you have access to all computation power on Earth, it can take thousands of years to run through all possibilities.

Chapter 17 Understanding Diffie-Hellman Key Exchange

For as long as we know, people have always wanted to keep secrets. It has taken a lot of time and effort to accomplish this. As I mentioned before, the use of encrypted data can date back to time immemorial. In 1976 Whitfield Diffie and Martin Hellman published a paper that explained how to create public key cryptography. They described a way of using open channels to exchange a secret key by using a one-way function called a discrete logarithm. As you can imagine, one of the biggest problems in cryptography, is to exchange the keys between two parties. We don't just want to establish a common key, but we want to do it in such a way, that anyone who is listening to the communication between the two parties, do not find out the key.

The problem: Imagine that Alice and Bob want to exchange the keys; though, Eve is listening to their communication and intercepts the key that's being sent between Alice and Bob. Unfortunately, if Eve gets the key, she can encrypt the data; therefore, that key would not be secured enough for Alice and Bob to communicate securely.

The solution: First, Alice and Bob would agree publicly on a prime modulus and the generator. Let's take an example using a Generator of 3, and a prime modulus of 17. Then Alice selects a private random number, say 15, and calculates 3 to the power of 15 mod 17 that would equal to 6. Then Alice would send this result publicly to Bob. Next Bob selects his private random number, say 13, and calculates 3 to the power of 13, mod 17 that would equal to 12. Then Bob would send this result publicly to Alice. If you are still with me, you might have realized that Eve might have captured both publicly submitted numbers that are 6, and 12; but, she would not know what to do with those figures so that she could carry on eavesdropping to the conversation between Alice and Bob. What happens next is Alice takes Bob's public result and raises it to the power of her private number to obtain the shared secret which in this case is 10. Bob takes Alice's public result, and raises it to the power of his private number, leading to the same shared secret. They have done the same calculation, even though it does not seem like it at first. Consider the following: Alice has received the number 12 from Bob, was calculated as 3 to the power of 13 mod 17, so her calculation was

the same as 3 to the power of 13, to the power of 15 mod 17. At the same time, what Bob did was this: He received the number 6 from Alice, and he calculated as 3 to the power of 15 mod 17. So basically, Bob's calculation was the same as Alice's which is 3 to the power of 15, to the power of 13. They have done the same calculation, and the only difference is that they have used the exponents in a different order. They both have calculated 3 to the power of their private numbers. Eve would not be able to find the solution because she would get stuck on a discrete logarithm problem, and with large enough numbers, practically impossible for her to break the encryption in a reasonable enough time. This is how the key exchange problem is solved without any interception whatsoever. Again, thanks to Diffie and Hellman.

Chapter 18 Elliptic Curve Cryptography

First you have to understand that Elliptic Curve Cryptography is significantly more secured than any other modern day cryptography functions. Like many cryptographic systems, elliptic curve cryptography gained its power in mathematics. Generally, the elliptic curve's form is the following:

$Y2 = X3 + AX + B$

A and B are constant values, they usually can be real numbers or rational numbers. Elliptic curves can be done using standard algebra; but, they actually require their own definitions for thinks like: addition and multiplication. Therefore, in order to understand how Elliptic Curve Cryptography works, you must understand first how Addition and multiplication works.

Addition: Imagine a curve that you are about to add two points to: one called A, another called B. Once you have added those two points, you have to draw a line between them. However, once you do that, you may realize that there is a third intersection on the graph. Once you have found the third intersection, you should begin to draw a new line and this new line, where it intercepts the curve again, will become your third point that you should call C.

Please note C is equal to A + B

$C = A + B$

Next, you can define the intermediate position on the top half of the curve which you can call X. This is very important because the Addition requires a third intercept point; however, adding two vertical points is an undefined procedure. Therefore, this results to what is called the Elliptic Identity, also known as Infinity. The reason for this is when you would try to add two vertical points, there would never be a third interception, and you cannot define that addition.

Next, consider adding a new point to itself: If you are adding a point to itself, of course, there is no second aspect to be considered, and you cannot draw a line between them. Instead, you can draw the line through A, and find the point where that would intercept on the curve. Once you have done that, it is the same procedure as before by drawing a vertical line, based on where the

line intercepted the curve, and the crosses will find point B. Note, B now equals to A + A. This is also known as Point Doubling. This is indeed a common way to achieve multiple occasion. This is also very similar to another algorithm called square to various algorithms, and if you repeatedly point double, you are doing what's considered multiplication regarding elliptic curves. Let's call this 2A and move on to think about what if we want to calculate 3A. To perform some multiplication with three times A, you have to perform point doubling three times, meaning you have to add A to itself three times. First, you have to draw the line between 2A and A, and wherever that line intercepts the curve, you flip across the x as you have done previously. As you can see, there is lots of jumping around, even just to perform a few multiplications. This computation is very similar to the square multiply algorithm, and this is where Elliptic Curve Cryptography gets it straight. As it's infeasible to divide the multiplications and find a particular point that you multiplied, unlike in regular algebra. For example, if you've been given the number 10, and someone says he multiplied 5 to give you the number 10, you would know that the other number from the multiplication would be 2. Yet, it doesn't work like that in Elliptic curves. This is also known as the elliptic curve discrete logarithm problem. To compute the multiplier point, you would need to calculate all the multiples of the given point until you would find the one that matches. Of course, this is not possible, especially when you use larger values; due to the computation complexity of this problem. Please understand that explaining fully what Elliptic Curve Algorithm is, could take a full book itself, in fact, books. However, I have tried to explain a general overview about this type of cryptography as it's used by Bitcoin, as well Blockchain technology. Briefly, Elliptic Curve Cryptography is one of the most secured cryptographic systems used today. It's computationally infeasible to calculate the private keys when using Elliptic curve key exchange.

Chapter 19 How to Encode arbitrary data

In this chapter, I will explain some basics on different encoding mechanisms that Blockchain uses for encoding arbitrary binary data into ASCII text; however, first let's begin with what ASCII text is.

ASCII: This is a character encoding standard, that represents text file to PC's, computers, and other telecommunication systems. ASCII stands for American Standard Code for Information Interchange. It has been standardized by IANA – Internet Assigned Numbers Authority. IANA is mostly known for controlling IP Address allocations around the world; however, that's an entirely other topic for a different day. ASCII has been used to represent English characters in the form of numbers as each letter assigned a number from 0 to 127, therefore, providing 128 possibilities. Computers are converting text into figures because it makes it possible to transfer data from one computer to another. The standard ASCII character set uses 7 bits, which is 27 = 128 possibilities for each character for English letters. However, there are many other character sets, such as SIO8859 or Unicode, using 8 or more bits to convert non-English characters and other symbols into numbers. To understand further how ASCII encoding and decoding work, it is advisable to see an ASCII table, so you can see what numbers represent each letter. I will provide an example for your reference, so you can further understand how ASCII encoding works.

Let's take an example of a word: "Hello"

If you began to encode the word Hello to ASCII text, the following number would be converted to:

Hello -> ASCII Encoding -> 72, 101, 108, 108, 111

At the same time, if you would want to decode the numbers back to its original letters, you would have to convert it as follows:

72, 101, 108, 108, 111 -> ASCII Decoding -> Hello

Please note, if you use the same word: hello. But this time the h letter wouldn't be written as capitalized, the ASCII encoding would give you a different outcome. In this case the word hello would be a number of:

hello - > encoding -> 104, 101, 108, 108, 111

BASE-64: This is a way of encoding arbitrary binary data into ASCII text. Base-64 encoding systems are commonly used when there is a need to encode binary data; for example, images or audio, that needs to be stored and transferred over media that are designed to deal with textual data. This is to ensure that the data remains intact without modification and any alteration during transport. Base-64 encoding schemes use both capital A-Z, lower case a-z letters as well 0-9 numbers for the first 62 values, and the symbols of + (plus), / (slash). The = (equal) symbol is used as a padding character. Base-64 maps are 3 bytes. (8 x 3 = 24bits) in 4 characters that span 6 bits (6 x 4 = 24bits). When the number of bytes to encode is not divisible by 3, and there are only 1 or 2 bytes of input for the last 24-bit block then extra bytes with value zero are added, so there are always three bytes.

BASE-58: Base-58 encoding schemes are also converting binary to base-64 encoding without using 0 (zero), O (capital O), I (capital I), l (lower case l), + (plus), and / (slash) because they look the same in some fonts. Base-58 is used in Bitcoin and is unique to the Bitcoin project. To apply the Base-58 encoding, you have to implement the same process like with the Base-64 encoding; however, instead of using the Base-64 symbol chart, you have to use the Base-58 symbol table.

Chapter 20 What is a Checksum

Some identification numbers have digits embedded inside their numbers. Some of these are well known to the public, such as bank account numbers. These digits can be numbers of characters that are called Checksum Digits, and are used for error detection if you mistype the identification numbers. Let's look at a British bank account number as an example:

GB29 NWBK 6016 1331 9268 19

In this example, the two-digit checksum values are 29. There is a special algorithm applied to this bank account number to calculate this checksum value. For example, if you would mistype this account number by typing:

GB29 NWBK 6016 1331 2968 19

Any British bank application will notice that this is an error because the checksum value of this number does not correspond to the expected checksum digit of 92, instead, 29. Most cryptocurrencies, such as Bitcoin, are also using checksum digits. To be fair, there are so many Blockchain implementations that it’s hard to say if all crypto currencies are using checksum digits; but, when it comes to Bitcoin, it is certain. What you have to understand is that checksum and hashing are not the same, in fact, there are some significant differences between them, so let me explain them. The checksum is designed to detect accidental errors in small blocks of data, such as: social security numbers, bank account numbers, cryptocurrency addresses, and so on, but they are most often very fast to compute. While a hash reduces large data to a smaller number, in a way that is minimizing the chance of accidents. Social security numbers or even bank account numbers are only identification numbers and have no other functions, but to identify individuals for Social Security or banking. However, the public key has a corresponding private key that is mathematically linked to each other. These keys are used to create a transaction between two or more parties, by using encryption, as well decryption, of data using these keys. The randomly generated private key and the calculated public key are converted into private addresses and public addresses. There are multiple reasons why the public and private key pair are turned into different looking public and private addresses, so let's look at some of those examples:

- Implement checksum digits in addresses to detect mistyping of the addresses.
- Perform version number in addresses to differentiate between similar Blockchain implementations or the environment.
- Apply Base-58 encoding to addresses to avoid mistyping of the addresses.
- Use the hash algorithm to addresses to reduce the address sizes.

Chapter 21 Understanding Vanity Addresses

A vanity address is a public address where the part of the address is chosen by the address holder. Basically, Bitcoin addresses that have a custom prefix within. To better understand let's take a look at a Bitcoin address.

1555JSudJlo9HYPLMbbriwoYdFQawszx6SBgIndkshhe

Here the vanity numbers are 555; however, you cannot start your Bitcoin address with the same numbers as every single Bitcoin address always starts with the number 1 as the first prefix. However, you might choose to have your vanity letters at the end of your address, like the example below:

1JSudJlo9HYPLMbbriwoYdFQawszx6SBgIndkshheCAR

To generate vanity addresses yourself, there are many platforms that you can do so; however, there are few things to note here. If you want to have vanity letters or numbers that are between one or three characters long, those addresses can be generated quickly. However, if you choose to have a vanity address that is four or more character long, the procedure could take as long as hours or even days to generate. It is not necessary to create a vanity address; however, I will provide some reasons why you might choose to use a vanity address.

- Branding: Vanity addresses can be ideal for organizations, as well improving brand recognition for businesses.
- Business model: You might choose to use some part of the address as services that you offer to your clients, for example using the word: CarHire within your address would stand out, making clients recognize your business as more professional than an average car hire service.
- Donation purposes: Again, same as using for business name or services. If you want to use a Bitcoin address for donation purposes, you may choose to reflect that within your address, so that it would be visible to those who transfer to it.

When the vanity address is generated, only the public key (also known as a Bitcoin address) is custom. The private key would remain random. In theory, the entire address can be custom; however, it is infeasible to generate an address with the prefix of over 6 or 7 characters. Some websites will create

vanity addresses for you; however, do not use any of them unless they use split-key generation incorporated. This function is where they would generate a public and private key pair, and you would give them the public key. Next, they would create a vanity address with your public key, as well another key pair. Using this technique, the service that would create a new vanity address would only know some of the private key needed to use Bitcoin. In case they do not use this technique, then it is possible that those services would be able to steal any Bitcoin stored on that address. Some issues regarding vanity addresses that are good to know. For example, as I mentioned, anyone can create a vanity address, that is nice. However, hackers—or anyone with bad intentions—might also know that fact and would try to use it to their advantage. What a black hat hacker would do is simple really: they could use your legit company or donation name within their Bitcoin address and try to receive funds by impersonating you or any business that has good intentions. Another downside, again, is that longer prefixes could take a long time to generate.

Chapter 22 Understanding the Double Spending problem

Blockchain is not exactly money but when you think about what money is, I am sure that you have to think carefully to answer to this question. There are simple answers too and having to define what money is using one word, and if you were thinking about the word “payment”, you are absolutely right! Money is a sort of payment in exchange for a service or an individual product. Now that you know that money is some kind of payment, let’s think about the value. Certain products have different values in different countries; and to separate boundaries and measure the values of each product to different countries, some regulations can be purchased and what not all over the world. Blockchain has no limits: as it’s running on top of the internet, which is accessible from anywhere in the world. However, when it comes to electronic payments, there are issues and a big one is double spending. Back in the early 80’s e-cash was conceived as an anonymous cryptographic electronic money. The way it worked, in a simplified explanation, is this:

Banks created an electronic money, that was cryptographically signed. The digital money contained a unique ID, also known as a token. Users were able to purchase these funds, then begin to spend it in shops. What happened was that e-cash was relying on a third party to get authorization, or some kind of proof, that the e-cash was valid, and it had not been spent previously. It sounds like it doesn’t make any sense; however, because electronic files are easily duplicated, banks were required to check on all e-cash to make sure they hadn’t been spent yet. The double spending problem is the main issue that needed to be solved to introduce a new electronic money system. The problem could have been solved by using a central trusted third party online, who could verify that the electronic cash has not been spent yet. Back in the day, the idea was that this trusted third party could be anyone like: a bank, broker, or any entity that can facilitate interactions between two sides who both trust the third party. Of course, there are plenty of disadvantages for trusting in third parties; in fact, in any financial services. In the 2008 financial crisis when several banks failed, it taught us there is no such thing as a trusted third party. They failed mainly because of mismanagement, or greed —or even many because of involvement with illegal bank activities. Additionally, half of the adults around the world have no access to financial services because financial institutions are too far away or too expensive to

use. Third parties are commercial entities; therefore, they will charge fees for their services. If you think about inventing a new electronic money, one of your goals should be to make it accessible to anyone around the world. Third parties have the power to suspend customers' accounts. For example, a few years ago PayPal suspended WikiLeaks donation account and froze its assets. PayPal claimed WikiLeaks encourages others to engage in illegal activity. This was not a result of legal process, but rather the result of fear of falling out of favor with Washington. Third parties can also deny or limit access to your assets. For example, in 2015 in Greece, the banks had limited access for cash withdrawal because of the rush on the banks. The solution for double spending without third parties now exists; and that is what Blockchain allowed for Bitcoin. Bitcoin was the first application to solve the double spending problem without the use of third parties, or any involvement with any centralized system. Satoshi Nakamoto came up with the idea of Bitcoin and created its original reference implementation. Therefore, Satoshi has solved the double spending problem using a technology that is called today Blockchain Technology. The system is based on cryptographic proof instead of trust. Blockchain technology was originally used as a cryptocurrency for the payment transaction between two parties, but nowadays it can be used for many other services such as:

- Notary Services,
- Identity services,
- Voting services, and more.

Chapter 23 What is the Great Ledger

The ledger is a sort of database where confirmed transactions are recorded. Traditional centralized ledger systems work in a very similar way as the Blockchain ledger system; however, there are few differences.

Centralized ledger: An old way of doing a ledger system that is centralized by a bank. For example, it works like this: if you purchase from me, you pay me; really, you would only initiate a transfer from your bank account to my bank account. Then both of those banks, if they are not the same, would have all the details of the transaction registered. Though, only those two banks would be able to access those transaction details, therefore, no other banks, nor anyone else, would have access to those details. If someone wants to have access to see the details, they need to ask the bank for authorization first. Of course, it all depends on what is the reason for the access. But the point here is that this traditional ledger system is still working in the same way. There are several different kinds of ledger systems; yet, when it comes to Blockchain's great ledger system, it's not centralized. It resides on the peer-to-peer network; therefore, it's a decentralized ledger system.

Distributed Ledger: Blockchain platforms do not use a centralized database; instead, each node has a copy of the ledger that resides on the peer-to-peer network. Cryptocurrencies, such as Bitcoin ledger, only store balance information in the distributed ledger. Nevertheless, other platforms can, in fact, are already storing other information. Blockchain platforms, such as Ethereum can store any information in the distributed ledger. Some examples are Identity information, patient information or Real estate information. This method is also known as a public ledger, or permissionless ledger. When there is no central authority managing access to the ledger, this ledger is called a public ledger or, again, a permissionless ledger. So basically, you, or anyone, could join to the existing peer-to-peer network (for free of course) and receive a copy of the ledger of all existing transactions that have ever been recorded on the Blockchain. This would date back to January of 2009 when the great ledger began to work for the first time. As you can see, this is completely the opposite of what the current banking systems are providing.

Private Ledger: When there is a central authority managing access to the ledger, it’s then called a private ledger, also known as a permissioned ledger. This is of course not a peer-to-peer network, and you would have to ask for permission from the central server to have access to a copy of the ledger. The Blockchain ledger is visualized as a series of blocks which are connected with each other. Each block is made of a header, containing metadata, such as its previous block hash, Merkle root hash, and nonce. Followed by a list of transactions. The blocks are connected with each other, by referencing each of its parents’ block hash.

Chapter 24 Comprehending the chain of Blocks

All blocks in the main chain are numbered, starting with the number 0, then 1, 2, 3, 4, 5, and so on. The green block is the first block that was created, and it's also known as a genesis block, and it has a block number zero. The purple blocks are the ones that are forming short and invalid chains, they are called Blockchain forks. Blockchain forks do occur very often, additionally these side forks, also known as orphaned forks. A Bitcoin block is created every ten minutes on average; however, Ethereum blocks are set up in every 17 seconds on average. The block height is the sum of the blocks in a chain between it and the genesis block minus 1. Blocks on side forks can have the same block height as blocks on the main chain. Particular nodes on the peer-to-peer network are creating these blocks. These nodes are called miners. All the miners are collecting every transaction that people are sending to each other over the network, and only valid transactions are relayed to the other nodes. Each miner takes a number of these collected operations and puts them in a newly formed block. These lists of transactions are numbered tx0, tx1, tx2, … and so on. Tx stands for transaction, followed by the number. The first transaction (tx0) is also known as the coinbase transaction. This is the transaction where the miner assigns a block reward to his address. This is how Bitcoins are created. For Bitcoin, the block reward is halved after every 210,000 blocks. Once there have been 64 halvings, the block reward will be zero. There will be a maximum number of 21 million Bitcoin in circulation in the year of 2140. Other Bitcoin transactions, such as tx1 or tx2, are the ordinary transaction where the Bitcoins are transferred from the owner address to a recipient address. Each transaction requires a small transaction fee. This fee will continue to increase as an incentive for the miners to create new blocks because the block reward will continue to be lowered. When the miner has constructed the block, he must solve a hash puzzle that is applied on his list of transactions. The miner who first solves the hash puzzle is allowed to broadcast his block on the peer-to-peer network. The block also includes the solution to the puzzle, also called the nonce, in the block header. This is, of course, available to anyone who wants to see it and the details for each block can be found at www.Blockchain.info Other miners on the network will receive this block, and they validate the block before they append it to their chain of blocks. It happens regularly that another valid

block is broadcasted on the network because another miner has solved the puzzle nearly at the same time. When this happens, temporary forks are created. For example, fork A and fork B. Let’s assume that 70 % of the miners on the network are working on fork A, and the rest of the miners are working on fork B. In this example, fork A becomes the main chain because it consists of the longest series of blocks from the genesis block. Miners should always work on the longest chain. In this example, blocks on fork B will become orphaned blocks. The miner who solves the hash puzzle, and his block is on the main chain, will receive the block reward and also all the transactions fees (tx1 and tx2) in this block. The miner who has solved the hash puzzle, and his block is an orphan fork, cannot spend the block reward and transaction fees, because his block is not on the main chain.

Chapter 25 Understanding Testnet and Faucets

Due to the scaling transactions, the original Blockchain that was created back in 2009 requires certain maintenance. Back then, there were only a few transactions; however, as of mid-2020, there are close to 150,000 transactions every day. That means more than 6,250 transactions within an hour, which comes down to 105 transactions in every minute, meaning nearly 2 transactions are happening every second. I hope you can understand that the system does require updates to make sure all those transactions can be handled by the network. There are already plenty of Blockchain jobs on the market, and if you have good programming skills, you could become a great Blockchain engineer. Blockchain developers are highly paid; a permanent Blockchain developer pay rate starts from 80K to 150K, even 300K per year. The problem is that only a few people understand Blockchain, as the knowledge of technicality required can be overwhelming and certainly not for everyone. Having a bit of knowledge on C++, SQL, or Python could be very advantageous, and if you are into learning these programming languages, it will pay off. Two decades before, everyone was on about that IT is the future, and learning such skills will be needed for most future jobs. It is certainly good to have some IT background, especially if you are planning to become your own bank; though, let's be specific for a moment. Learning IT skills can mean many things; so, you should be specific, and specialize. I can easily say that the future jobs that will pay off big time are software developers, or to be more accurate, Blockchain developers. Where to start? Get an online course on Python programming for beginners, along with a reference book. But before I start a whole new topic on programming skills, let me explain a little bit about what environments current Blockchain developers are using for testing purposes.

A testnet is an alternative Blockchain used by developers for testing purposes. The crypto coins mined on the testnet, also known as testnet coins, have no real value. A testnet offers developers a sandbox environment to experiment without having to use the actual crypto coins or worrying about breaking the main chain. The main chain is also called, the mainnet. In case you we're wondering about mining Bitcoin, this is it. You can quickly mine your own Bitcoin or Ethereum testnet coins by setting up your own Bitcoin or Ethereum node. There are fewer miners on the testnet, and the hash difficulty

is also low enough to find solutions easier for solving hash puzzles—as well —getting a block reward. The mainnet and testnet are two individual networks, and there is no availability to send coins from one platform to another neither vice versa. To work on the Bitcoin testnet, you need to generate a differently formatted testnet Bitcoin address. A Bitcoin testnet address always begins with the letter m or n. The Bitcoin testnet address does not work on the mainnet. However, when it comes to Ethereum, there are no differences between testnet and mainnet. The same address will work on both networks: testnet as well mainnet. Therefore, you must be very careful not to mix them up. There is another way to get testnet coins, and that is to search for a Bitcoin faucet or an Ethereum faucet. A faucet is a website that dispenses small amounts of testnet coins on your address in exchange for completing a task described by the site. You can easily google search both: Bitcoin faucet, or Ethereum faucet.

Chapter 26 Segregated Witness

As I just explained some testing tools for developers, let's see what else is out there that requires maintenance when it comes to the real Blockchain network. SegWit stands for Segregated Witness. SegWit can be explained in many ways, and its technical details can be very confusing for some; therefore, I will try to explain simplistically before really diving into it. SegWit is a change on the Blockchain network, more specifically it's a change within the blocks. I am a network engineer, and it's easy to say, that when it comes to a decision of making a change, especially within the production environment, it is because there is an issue that needs to be addressed. The problem currently with the blocks is simple. Each block can handle 1MB of data, meaning all transaction details. Once there is enough data within a block, the block gets sealed, and miners start to create another new block. The issue that needs to be addressed is that each block gets filled with some data, but indeed it has been identified that there should be more data within each block. I have explained previously that each block contains lots of data, in fact, every transaction details are recorded on the Blockchain, specifically, within the blocks. Data such recorded are the block number, destination address, source address, transaction value, hashing algorithms, and so on; however, one of the most important data recorded, is the actual script that contains the digital signatures as well the public keys. To have a block validated on the Blockchain peer-to-peer network, these parts of the Blockchain rules had to be within the script. Nevertheless, it has been identified that the current situation is slowing down the system, and an upgrade is required. This scaling issue needed to be addressed; therefore, Blockchain developers came up with an idea. The solution is called SegWit. But, the real plan to implement SegWit is to remove the script from the blocks, making the blocks lighter; therefore, leaving more space for additional transactions, as well, speed up the system. Though, the proposal has a possible side effect. The reality is that the script is still going to be required as the rules of the Blockchain cannot be changed, therefore, part of the proposal is that there will also be an extended block that will have the script. This is of course very confusing for many, especially for those who have no technical background. The other problem is that developers were not sure if it's going to work out ok or not: even though they believe it is needed,

hence the change proposal in the first place. SegWit was implemented on the 23rd of August 2017 successfully. This deployment was a solution for many other issues too. One is that each transaction fee is very cheap; but, it could be even less expensive. What you have to understand is that Bitcoin is an excellent digital currency when it comes to values such as $100 worth or more. But, in order to implement it worldwide in every store, it requires some upgrades. For example, if you make a payment using Bitcoin that's worth $100, the transaction fees could cost you around $0.30 cents. But, when you want to buy an espresso from your local coffee shop that costs a dollar, a $0.30 cent transaction fee could be just too expensive. So, what has been identified is this: If we could add more transactions to each block, like twice as much, that could mean that each transaction would cost half of what it is now. Nevertheless, in order to fit more transactions to a block, something has to be removed. What has been discovered, is that the script can be re-written and added to an extended block on the original block, and this would be called Segregated Witness aka SegWit. But, why is this technology called SegWit? Well, the witness is also known as Cryptographic proofs, and the signatures that are used are also witnessing the proofs. Separating the signatures from both the transaction data structure and the block data structure into their data structure. Taking the signatures out of the transaction data structure is the main reason; still, there are some side effects, so let's take a look at them. First, side effects are not always bad, in fact, regards to SegWit, there are some very positive outcomes possible. The original goal was to clean up some of the functions of Bitcoin. One thing that is not static within the transaction data is the digital signature. To be fair, everything else is covered by the signature, therefore, cannot be changed effectively, unless invalidating the signature; yet, the signature itself can be malleated. So, once the signature would be taken out of the transaction data, the transaction ID would not be based on the signature anymore. The transaction ID's hash is not based on the signature, which means that the transaction ID cannot be malleated. This, in itself, was a massive development, and it helps with chaining transactions. Additionally, it helps with lightning networks, as well payment channels and it resolved lots of problems that we had with transaction malleability.

Chapter 27 Transaction malleability

In simple terms, transaction malleability is a cork in Bitcoin, and other cryptographic systems, where you can make unauthorized changes to transactions and re-broadcast with a different transaction ID. You cannot change where the funds are coming from, neither where the funds are going, because the signature covers that; but you can make small modifications to the signature. Let’s think of this in simple terms. Let's say that the signature contained the number 5. The analysis of the algorithm 5, and 05 are the same, but if you pad a number in a certain way, it will change the fingerprint of that transaction, even if that signature is interpreted the same way. Therefore, you can modify part of the signature because they are not covered by the signature and they would produce a transaction with an entirely different ID. By doing that, you can jam it into the network and cause confusion. Transaction malleability has been blamed for some thefts and Bitcoin exchanges, where people mostly are getting a form of double withdraw, using transaction malleability. It also allows you to carry out a DOS – Denial of Service Attack, against the network; as well, against the people who are using payment channels or chaining many transactions together. But, how does SegWit allow more transactions on the network? One of the interesting side effects of SegWit is that you can start counting block sizes differently and give some capacity to increase directly through the SegWit. Transactions are the key to opening the door to get into the Blockchain; therefore, you need a signature on the transaction to be validated to the Blockchain. Nevertheless, once the transaction is in the Blockchain, nobody checks those signatures ever again; typically we do not go back to see old transactions that happened a long time ago. They’re only buried within the Blockchain. They have been validated: therefore, old transactions are already trusted. The signature is only used once for validation. For example, when you write a paper check, you have the option to go to your online banking system and look at the image of the check after it has been submitted and cashed. It's not part of the bank statement, and you don’t need it for anything other than to check it once to see that it was validated; after, it's only hanging around, no need for it anymore. Same thing applies to signatures. What you have to understand is that digital signatures take 75% of the total space of some transactions. Additionally, the more transactions there are, the bigger the signature gets.

Large complex scripts and multi signatures have huge signatures, and they take up a lot of space on the Blockchain, and, again, nobody ever cares about them once they have been validated. The other part of the SegWit wasn't considered until recently because fixing malleability and removing transaction signatures from the transaction data is something that requires considering the whole network, and it's been assumed that it needs a hard fork. Though, there is a way to proceed using soft fork instead of hard fork. Indeed, it's a fascinating trick. This method allows you to put a version number in front of the Bitcoin script. What that does, is allows you to upgrade the version number of the script, while old clients cannot see the difference, but still able to validate transactions entirely. Former customers can continue to operate without upgrading, and all that is different is that they are endorsing a little less they used to do before. Additionally, new clients can upgrade scripts. Once you have a new version of a script (this is remarkable) as you can introduce endless amounts of soft forks parallel to change all kinds of scripting mechanisms. This trick is not only good to use for SegWit, but all other kinds of new developments. This is accelerating the innovation in the scripting language. Altogether these aspects: Segregated witness, Transaction malleability, increasing the capacity of the block by removing lots of information that's not used after validation, and the same time upgrading version scripts—make a truly compelling feature and resolve lots of problems.

Chapter 28 What is a Soft and Hard fork

First of all, let me explain a little about soft fork activation. It is usually done by a voting process, yet there is another innovation that is called Version Bits, also known as BIP 9, that was introduced in parallel and allows you to have multiple soft forks. What it allows you to do is say if a certain bit in the version of the block set, meaning you want to implement this soft fork, the miners then set that bit. Once 75% of the blocks have that bits set, you are activating the feature, then once 95% of the blocks have the bits set than that feature is forced for validation. It's a two-step voting process. It has been done on multiple occasions, such as Check Lock Time Verify. These incremental features can be voted on parallel. Previously, they had been implemented by increasing the blocks and by upgrading block version. For example, updating block version 3 to block version 4, and so on. Nevertheless, now you can turn the block version into a block field; therefore, you can do all these in parallel. Previously, it was that only one soft fork could have been implemented at the time, and the vote had to be completed by the way. It is hard to accept one, dismiss another, and move to the next. On the other hand, with the new proposal, you can implement multiple soft forks simultaneously. The important feature of the soft fork is that it’s forward compatible. In simple terms, let me provide an example for better understanding. Imagine that you want to open an old Microsoft word document. Word 1998 documents can be opened with the current version of Microsoft Word. This is what backward compatibility is, meaning it recognizes old formats. On the other hand, forward compatibility is when the version of Microsoft Word from 1998 that has not been upgraded would still open a document that we use today, or at least in a certain way. It may not be able to see all original details correctly, and may not be able to understand some of the features; yet, it still would be able to open the document. Therefore, soft forks have forward compatibility, meaning that clients who have not yet upgraded to the new code will not break and won’t stop validating so they can still maintain validating on the current consensus chain. All there is, is that they are validating less information because they may not be able to see the new features; still, they can ignore them while validating. Hard fork, by comparison, means that if you do not upgrade, you can no longer approve blocks, and you are no longer part of the consensus

chain, therefore, if you don’t upgrade, you are not on the network. There are always risks, especially when looking at compatibility. As I mentioned before, any change to the system apparently will cause effects. Soft forks, hard forks, they all have bugs, even though all these features are always tested on Testnet. For example, segregated witness testnet had been running for months before implementation, and that allows to have more faith before any change. Miners have become very concerned about any change and making sure there are multiple tests before any implementation takes place. The general belief is that soft forks are less dangerous than hard forks, but the problem that some people identify is that they do not force the network to upgrade, meaning you can end up with lots of old clients that validate less transactions. Nevertheless, some other developers prefer to have more of a strict approach, and just believe that if you don’t upgrade, you should be off the network. Therefore, it’s more like a philosophical issue rather than technical.

Chapter 29 What is Lightning Network

Lightning network is a Layer 2 network, also known as Data Layer network. It aims to scale peer-to-peer networks from millions to billions of transactions per second, simultaneously using smart contracts. For example, getting paid not monthly nor weekly, but every second. Exciting, right? I'm sure you would love that too! Imagine checking your online pay slip and seeing it always changing, showing you a different amount every second. But first, let's look at why the idea was born in the first place. Receiving payments monthly is obviously ridiculous. I used to get paid weekly before and that's a lot better; though, I've also had many jobs before where I used to get paid daily. Getting paid daily is what I most liked; yet, I was on a cash to hand basis, and it was not recorded anywhere; therefore, I cannot account for those days. Using Blockchain, especially lighting network, can allow you to receive validated payment simultaneously, which is registered in the great ledger forever. As an employee, I believe it's a nice way to get paid; though, think from an employer point of view. Imagine that you have a company that employs thousands of people. Each month people are working on pay slips, making sure everyone will get paid correctly, and still before any validation, it has to go through the bank, in fact, many banks, to get everyone paid. Therefore, lightning networks will be the favorite of every employer. Now that you have a good knowledge of how Blockchain and Bitcoin works, when it comes to lightning networks, it's actually bending the rules a little bit. Let me explain why: we know that when we send a Bitcoin, we broadcast the transaction, then we have to wait for confirmation, and confirmations are only arriving every 10 minutes in the form of a block. Once the block has been created, it groups many transactions, and it will get registered on the ledger. Nevertheless, if you are waiting for the next confirmation, you have to wait for the next block to be validated, that might take another 10 minutes. Because a lightning network works on top of the existing system, only using a different layer, it has its own layer for instant payment. The Lightning network promises no fees on the transactions. Again, this is new, simply because each transaction has fees that sometimes are even larger than the previous transactions were. Fees are for making your transactions a priority within the list of other transactions. The more fees you would pay, the faster you would get the confirmations. Paying no fees sounds like you are possibly

never going to get confirmed by the network. You must think of it in simple terms. Imagine when you go to a Pub where the waiter tells you that you have to pay cash, or if you choose to pay with a card the minimum order has to reach $5. This is because for each transaction the pub needs to pay a certain fee to the provider. Yet, if you open a tab, and you pay only once, in the end, there will be only one transaction fee that requires payment. When you create a payment channel on the lightning network, you have to deposit a certain amount of Bitcoin. Now you are proving ownerships for those Bitcoins by handing them over to the network. It also works with multi-signatures. The system has a way of enforcing these sets of rules; therefore, you don't even have to wait for the block to be confirmed. Once the transaction has been announced, it's is immediate; hence, you don't have to wait until these funds are approved. As we do not force the miners to write these transactions on the Blockchain, as normally, you would have to pay the miners for transaction fees. This system allows you to make many payments; still, you only have to broadcast it when it's necessary. It is highly complicated to implement and any bug in the code can cause a catastrophic outcome; thus, there is not a fully working resolution yet.

BOOK 2

BITCOIN FOR BEGINNERS

LEARN FAST WHY BITCOIN IS THE INVENTION OF THE 21ST CENTURY

BORIS WEISER

Chapter 1 The importance of cryptocurrency

Before I get into Bitcoin basics, I would like to point out that often people talk about Bitcoin but one might be thinking about the currency while another person is talking about the underlying network. Both called Bitcoin, but they supposed to be written in a different way. When Bitcoin is written with the capital B, it is referred to a Bitcoin network, yet when it's written like bitcoin or bitcoins with no capital letter used, it is referred to the currency unit of the network. There is no biggie if you made a mistake before, I personally often misuse it too, but I wanted you to be aware of it, as it might become useful to you one day. In case you find yourself in a situation where it is not clear, you can ask always ask if they referring to the currency or the underlying network. Anyhow, most people know Bitcoin as a cryptocurrency. Why is that? The first part of the word: crypto is really coming from cryptoghraphy, while the second part currency, sure enough, it can be used as a currency. Cryptocurrency is a digital currency where cryptographic proofs used for validating transactions, instead of trusted third parties. Unfortunately, many people still confuse digital currencies with cryptocurrencies, and the actual difference is really about cryptographic proofs. Basically a traditional digital currency does not use cryptography and that's is why it's just known as a digital currency. When it comes to transactions, using traditional digital currencies, the validation process relies on trusted third parties. The term, trusted third parties, they are referring to banks, or other money transmission businesses, such as PayPal, Payoneer, Stripe or even western union. They play a key part in our financial economy, but these companies are for-profit organizations, so when we use their services, they will change for a certain fee. It might be a transaction fee of a certain percentage, like 5% or 10% of the amount of digital currency is transferred, but it can be a flat fee too, for example, or if you make a transfer of 10 dollars, or 1000 dollars, the flat fee is always 5 bucks. There are other fees that you can get charged too, when it comes to international transactions, for example if I pay for an online course that is 200 dollars, and I am wiring money from my British bank account, I will get charged for currency exchange fees. For example PayPal is great because making international payments are extremely easy. All I have to provide is an e-mail address of the recipient, click ok, and done. But in the other hand, I get charged for a transaction fee, which is now a flat fee, and a

currency exchange fee. So what better way there is then trusted third parties? The answer is Cryptography. Cryptography has been used ever since thousands of years, and the main purpose of cryptography is to encrypt messages, so it can be decrypted only by those it was intended to, so for any eavesdropper, would be unreadable. Eavesdropper, I mean any listener, observer, anyone who would spy or capture the message. Encryption used by the sender and decryption used by the receiver. The most common encryptions are Symmetric and Asymmetric encryptions. Symmetric encryption is similar to a typical door lock, where the same key used to lock, as well to unlock the door. When using asymmetric encryption, we use one key to encrypt the message, and we must use a key pair, another key to decrypt it. They are known as private and public keys. When it comes to a Currency, it is basically a system of money that's in general use, also known as legal tender, cash, paper money or medium of exchange. Through the history we always had finance which mostly was controlled by governments or trusted third parties, while technology on the side had nothing to do with finance, but because of this technological breakthrough, we were able to combine finance and technology, and create something that we should describe as the invention of the 21st century. Bitcoin is not only a revolutionary fin-tech invention, but the only real medium of exchange in a form of cryptocurrency that received its value from the market, from the actual people who using it, instead of receiving its value from a King or any government entity like any Traditional printed paper money. Of course it's wasn't always like that, so in the next chapter I will talk about the history of money, and how we ended up with Bitcoin.

Chapter 2 Defining Money aka Medium of Exchange

In this chapter, I will focus on what money is, forms and types of money, and the history of money. First and foremost, we should ask the question the origin of money, and how old money is, but the fact is that no one actually knows how old money is. Researches show that money possible old as human civilisation, so if you think about it, in the past there were no bank accounts, or dollar bills. Money is defined as a medium of exchange, and back in the early ages, people realised that the most important requirements for human survival is: air, water, and food. Air and water in most places are free, but to get food daily, such as fishing or hunting it's a challenge. Slowly food has become a medium of exchange, and even today, some places food is still used as money. Time moved on, but really wasn't long, when people realized that food is not very good money, because it uses its value quickly. For example fruits, such as apple, banana or even any kind of meat have an expiry date, and once they are consumed, the value completely disappears. The solution were needed, something that could replace money for something that it's value would last longer, and people began to use rare objects in exchange for food. Rare objects were varied, as well their value in different locations, but we learned that commonly used items were see shells, rare stones, or precious metals, such as gold or silver. Especially gold become very popular amongst other precious metals, and it became wildly used as money. Gold has grown in popularity and the gold rush started in the 19th century and it lasted until 1980. Gold become more and more difficult to mine, which was good in terms of scarcity, but to maintain its value as a medium as exchange, in today's fast growing modern world, just cannot succeed. The problem with gold is that is heavy, difficult to divide, difficult to validate by an average person if it's not fake, and it's also difficult to store. Transportability also doesn't help Gold to become better money, as it's slow, too many people required for transportation, as well various security checks, which bring to the next point of confascatability. Gold can be easily confiscated, especially because it's difficult to store and difficult to secure. Gold hasn't got to many good use cases, other than jewellers, store of value, and not so much as medium of exchange anymore, and due to its scalability issues, amongst other issues, it had to be replaced. When the original paper money was introduced, it was backed up by precious metals such as Gold. Still, people didn't like the

idea first. It started in 1600 in the City of London, UK, and continued in 1800 by Napoleon in France. Times moved on, while people became confirmable using paper money, and slowly, Fiat money got introduced. The Fiat Money was introduced by the central bank in the United States, which is backed by nothing, except a trust and believes of the central bank, so since 1971 there is no gold backing paper money. By the end of the 20th Century, fiat money dominated nearly every country in the world. There are many problems with Fiat money, and one of the main issue is that is easily counterfeited, and because it's continuously injected to the market, it causes very high inflation. Transferring paper money also difficult so SWIFT was introduced in 1973, using a Plastic Card as a new Digital currency. SWIFT Stands for Society for Worldwide Interbank Financial Telecommunication. One of the most well-known SWIFTS ARE: Visa Debit, Credit Card, Debit Card, ATM machines, and so on. The swift digital system is basically a centralized messaging system between banks, currently operating with more than 20 million transactions per day. The visa system is still the fastest payment method in terms of handling transactions, which is capable of processing 24000 transactions per second. Swift is a great invention, but there are some fundamental problems with it, as it still requires Human administration in order to validate transactions, due to the double spending problem. In the next chapter I will talk about double-spending problem and its solution.

Chapter 3 Trusted third parties & **Quantitative easing**

Before talking about double spending I wanted to give you a better idea about trusted third parties from another angle. Trusted third Parties generally trusted by the people. For example you can purchase a product from a certain website via PayPal, and if you are not satisfied, PayPal can help you get a refund. On the other hand, trusted third parties are Commercial Entities and always charge fees for providing their services, which I have talked about before. They are also capable of suspending costumer's accounts, but they can also deny transactions or even limit access to our assets. For example recently, in 2008 when we had a Financial crisis, also known as Credit crunch, caused by massive housing bubbles, because of the banks sold a so called "TRIPLE A" rated mortgages, multiple banks and Financial institutions have failed. They were unable to pay out customer's money, because there was no money left in the banks, simply because they have managed to lend out to mortgage owners. The large percentage of these mortgage owners eventually lost their homes, because they were unqualified in the first place to have a mortgage. Another recent example was in Greece in 2015, when the Greek banks have announced limited cash withdrawal to their customers. There are other occasions, and places when the similar issues happened, but the bottom line is that Over 2 Billion people on the world are unbanked. People either unqualified to have a bank account, or they just leave too far away from a closest bank, but maybe they just find banks too expensive to be used. There are many other examples in other countries when trusted third parties failed, like Zimbabwe, India, Venezuela, Italy, even Hungary, were money became completely useless, due to its inflation, caused by quantitative easing. Quantitative easing, is a term used by governments or the central bank, when money injection required to an existing system. The central bank, also known as federal reserve, or but most known as the FED. If you watch news channels, and see a representatives of the FED, they don't say quantitative easing, instead they say sentences like:

''We recommend to implement QE to solve issues with the current economy''. What they mean in plain English is that '' we have to print more money, and bail out all the greedy banks, so they can continue lending out money for profit''

Fed was always printing money ever since the 70-s, but they really began in

2008, by printing 600 billion dollars, so they can buy mortgage backed securities, but, by the end of 2009, they had 1.75 trillion dollars' worth of debt. This is of course crazy, but the fed announced a second round of QE, in November 2010, by creating another 600 billion dollars, which was referenced publically as qe2. In 2012 September the fed announced qe3, lunching 40 billion dollars every month, even received a nickname of "qe-infinity", because it was an open-ended announcement, but it got worse 3 months later, when they changed the printing of 40 billion, to 85 billion dollars per month, which continued till end of 2013. In January 2014, the fed ended up having 4.5 trillion dollars in assets of debts, meaning they been printing about 4 trillion dollars within 5 years. There are plenty more to discuss about the FED, how they print money, how money comes to existence, but in this chapter just wanted to give you a high level overview of the current monetary policy.

Chapter 4 Double Spending Problem & Solution

In this chapter, I will define what double spending is, why it is possible, and how we solved it. First and foremost, double spending is only possible with digital cash, or digital files. For example by sending the same digital file to multiple recipient in the same time, like emailing a digital picture, like a holiday picture you have taken with your phone to multiple people, you are doubling, in fact tripling the digital file. But there is also another issue, which is that you cannot prove me that you don't have that file anymore. When it comes to digital currency, this is possible because a digital token is a digital file that can be duplicated or falsified. Because there is no automated validation process, like the Bitcoin blockchain has, in order to avoid double spending with traditional digital cash, we need trusted third parties to validate transactions on the SWIFT network. In 2008, a decentralized distributed system was proposed by Satoshi Nakamoto. Satoshi has published a white paper which he called: "Bitcoin: A peer-to-peer electronic cash system". This system was implemented in January 2009, and which we know today as the Bitcoin network, which is based on the technology called the blockchain, and it's currency called bitcoin. The Bitcoin-Blockchain has solved the double-spending problem by using cryptographic techniques for transaction validation, instead of trusted third parties. In the case of Bitcoin, each transaction will stay in the unconfirmed transactions Pool. Then, while each transaction getting confirmed, only the first transaction will be validated. This is why it's recommended to wait 6 confirmations until considering a transactions complete. This method also known as proof of work, as there is no human administrator required, instead, computation power solves puzzles for validating transactions. Due the this process, the blockchain technology eliminates the need for trusted third parties and human interventions while we can transfer bitcoins from point A to point B. I will get into more details of the bitcoin creation, bitcoin mining, transactions, and blockchain basics shortly.

Chapter 5 The revolution of Crypto & Digital Cash

DigiCash

It is important to understand that Bitcoin wasn't just born out of a thin air, instead, you must be aware that, before Bitcoin, there were many trials and errors. In 1982, the paper was written by David Chaum, a computer scientist and cryptographer, also a Cypherpunk, where he defined his design to a new electronic cash, which he called: DigiCash. David has implemented the DigiCash system in 1990, but the First DigiCash Transaction has only taken place in 1994. This system has allowed users to obtain digital currency from the bank, which was untraceable by the bank or any other third party. Unfortunately, DigiCash filed Bankruptcy in 1998, and even if this company was only active for few years, the idea of DigiCash was the technical root for the Cypherpunk movement where the idea of Bitcoin was born. Moving to the year of 1996, E-gold was born.

E-gold

E-gold was referred to Digital Gold Currency, implemented by Douglas Jackson and Barry Downey. They have backed up services accounts with Gold or other precious metals, stored in a Bank safety deposit Box in Florida. This has been going well and by 2004 they had over a million registered accounts. People mainly used E-gold for trading precious metals, online auctions, or online casinos, and it was also used by many political organizations, even non-profit organizations. A year later, E-gold was facing issues because it was used by criminals for money laundering purposes, and other criminal activities, and the company was raided by the US Feds in 2005. In 1998 Nick Szabo designed a digital currency, which he named: Bit gold, which was never implemented, but the actual framework has many similarities to Bitcoin. According to Szabo, Bit gold still would require trusted third parties; therefore he called it an unaccepted solution and left the project. Bit gold however, has been called a forth father of Bitcoin by many cryptographers. As I mentioned earlier, there were many trial and errors, and because most Cypherpunk members couldn't create a decentralized system for digital cash, they stopped working on the idea. Nearly a decade past until an anonymous person or persons called himself Satoshi Nakamoto, began appearing on the cryptography mailing list and other Cypherpunk related

websites. In October 2008, Satoshi Nakamoto has released a white paper which he called: “Bitcoin: A Peer-to-Peer Electronic Cash System”. On the 3rd of January 2009, the system went live, and it’s online ever since. One of the many reasons the Bitcoin network is still online is because it became the most decentralized peer-to-peer network and continued doing so. The system was implemented, so there is no central point of failure, therefore the first ever cryptocurrency was born, running on a Peer-to-Peer system, based on cryptography. Finally the dream of the Cypherpunks, after 2 decades has now arrived, bright by Satoshi, in a form of Bitcoin. Bitcoin was the first with its decentralized payment system, but there are plenty of famous centralized payment systems as well, such as the swift system, with credit or debit cards, PayPal, Payoneer, eCash, stripe, Apple Pay and many others. Once again, when it comes to Decentralized Payment Systems: Bitcoin was the first, and because it’s an open source project, anyone can take a look at its code, copy it, make multiple versions if you wish to because it was released under MIT Licence. The problem with the MIT licence was that lots of people began copying it, and started creating their own cryptocurrencies such as Ethereum, Litecoin, Zcash, Dash, Monero, and hundreds; in fact there are thousands more. What most people don’t realise when it comes to cryptocurrencies, is that most of them are under a certain authority, and completely centralized.

Chapter 6 Centralization and decentralization.

Before talk about the key differences between centralization and decentralization, we should understand what Authority means. Authority means, that we give away our power to a person, or company to hold other people accountable for their actions, and the right to make decisions about the use of organizational resources. This is indeed a very confusing definition, so let me explain in plain English by providing an example of how a centralized network operates. In centralized networks or companies, the top management decides who can participate in the network, or who can work for the company. There are restrictions, and only selected people can access certain details, and these people normally chosen, or allocated by the management. When it comes to a problem that an employee unable to solve, it is solved by the managers, or has to be solved by following company standards, or managers decisions. Regards to software updates or any kind of changes in a centralized system, once again it's decided by the top managers. Given that, if you look at how each bank operates, you can see that all banks having their own centralized ledger, and they don't share amongst other banks. For example, if you have an HSBC bank account in the past 20 years, they do have your personal details, as well your transaction history, but any other bank would not know any details about you whatsoever. This is also the reason that trusted third party is required, when you make a transaction to another bank account, as each bank has its own ledger system. Decentralized networks, in the other hand are also known as Peer-to-Peer Networks, where anyone can participate by their own will, and the same principles apply if anyone wants leave the network they can do so, at any given time. For example, in the case of the Bitcoin network, anyone can join by downloading a free software called "Bitcoin Core", you can start validating transactions immediately, without asking any permission from anyone. In decentralized networks, there are no managers, there is no authority above another, and the Problems solved by the workforce together, where anyone can have an opinion. So, when it comes to software updates in a decentralized system, it is the decision of the Bitcoin community, achieved by voting. The Great Ledger is shared through every Bitcoin node where the transaction validation is done by a shared, decentralized computation power, using cryptographic proofs. Couple of things to point out, that you should take away from this

chapter. First of all, I heard multiple times people saying that Bitcoin is completely decentralized, but it's not correct. The Bitcoin network is built on existing TCP/IP protocol, even if it's a peer-to-peer system, it is relying on internet service providers, ISP-s, and they are providing the underlying infrastructure. ISP-s are centralized entities, but because there are so many networks around the world, turning the whole internet off, is nearly impossible. I have done some research on how many ISP-s exists on the world, and there is no exact figure, but it is estimated that in the beginning of 2020, there were no more than 50,000 ISP-s but no less than 10,000 ISP-s. As you see this is a large range, so even if they are all centralized companies, to shut them all down, it would be very hard, and not even going to mention the possible consequences. So the Bitcoin network is not completely decentralized, but the most decentralized network, that exist today. In relation to centralized entities, I also want to point out that centralisation is good, and employees should follow company standards to provide the best customer satisfaction. But when it comes to money creation, history shows that centralized companies never accomplished harmony. Instead, what we learned from history is that each time when a human has a possibility for creating money, it leads to greed, power, and control. If we want humans to create money, we already have the Federal Reserve, which is a of course a centralized company. To finalize it, decentralization is highly inefficient, but in the case of Bitcoin it it's perfect, because there is no leader, no Bitcoin boss, there is no one who could take control over the network. I hope it makes sense, and you can differentiate advantages, and disadvantages between centralized and decentralized companies.

Chapter 7 The rise of the Cypherpunks

Many people don't learn history, and often say thinks like Bitcoin is a scam, or it's been created by the government, or by the NSA. But once you understand the intentions behind the Bitcoin creation, you will realize, this project is absolutely not a scam, and certainly not been created by any government entity, instead, it's all began with the Cypherpunk movement. Please don't confuse Cyberpunks with Cypherpunks. Cyberpunks were the ones used to listen techno music and partying for days, while the Cypherpunks are cryptographers, and their name is coming from a word: CYPHER which is related to Cryptography. So who are these mysterious Cypherpunks right? Well, before the Cypherpunks, until 1970, Cryptography only been used in secret operations by military and spy agencies. The first publically available cryptography was called: Diffie-Hellman Key exchange in 1977, named after Whitfield Diffie, and Martin Hellman. The Diffie-Hellman key exchange is still used today by most banks, and financial institutions. Moving ahead with 3 years, David Chaum came up with an idea he named DigiCash in the 1980's, and the roots to the Cypherpunk movement has began. More than a decade past when The Cypherpunk movement has began properly, when Tim May, Eric Hughes, and John Gilmore, started the Cypherpunk mailing list in 1992. It was a successful launch , because by they had more than 700 subscribers, by 1994. The Main discussions were: online privacy, cryptography and the concepts of anonymity. The Cyperpunks Principles were the following:

"Privacy is necessary for the open society in the electronic age, we can not accept governments to grant us privacy, We must defend our own privacy, We know that someone has to write a software to defend our privacy… and we are going to write it."

The Cyperpunk mailing list contained hundreds of people, still, they had plenty of projects in mind, most of them only made it to a design phase, stayed incomplete, unfinished project. Of course there are many notable achievements accomplished by the Cyperpunks, and I will list a few, such as:

- PGP for e-mail privacy – where Hal Finney was the main Author.
- BitTorrent – Created by Bram Cohen

- TOR Project for Anonymous web browsing
- OpenSSL – a Software library for web security
- Counterpane Internet Security by Bruce Schneier
- Smart contracts and the Bit Gold project, by Nick Szabo
- WikiLeaks by Julian Assange
- Blockstream for Bitcoin side applications by Adam Back
- And of course the Bitcoin design, and the invention of Blockchain technology by Satoshi Nakamoto

There are many more projects accomplished other than these, and most of the projects were accomplished due to a teamwork, and not as an individual achievement. In this chapter I wanted you to know that the idea of Bitcoin was originated from the Cyperpunks and not from the government.

Chapter 8 The MAN of the 21st Century!

Satoshi Nakamoto, who invented Bitcoin, also implemented blockchain, and deployed the first ever decentralized digital currency, known today as cryptocurrency. In order for Satoshi to succeed, he had to find a solution for the double-spending problem. The double spending problem relies on easily copied digital files, so he created a consensus system that is capable of auditing digital files, by eliminating trusted third parties. Satoshi not only solved the double spending problem, but found solution for the Two Generals Problem, aka Bizantine Generals Problem, by implementing the blockchain technology. Satoshi Nakamoto, is a sudoname of a person or persons, who has managed to stay anonymous since 2008. When it comes to Satoshi's timeline, the actual interaction with people that he ever made only lasted about 2 years. Through those 2 years, nobody has ever met him personally, neither talking to him over the phone, skype or any other type of voice call. There are close to 100,000 worlds can be found publically, that's been written by Satoshi, which help us conclude his personality. He uses a Japanese sudo name, while having a German e-mail address, but only communicating in English, and often uses British expressions, but that's not always the case. In order to create the Bitcoin network, Satoshi had to be an expert in several fields, such as: C++ programming, decentralized databases, peer-to-peer networking, monetary policies and economics, game theory, and of course cryptography. Because of these skillsets, there are many speculations that Satoshi is a sudo name for a group of people, or at least a small team, but considering what we learned from his well-structured writing style, it suggests that he is an individual. When it comes to the possible candidates of Satoshi, I heard all sorts of theories and speculations around Dorian Nakamoto, Charlie Lee, Craig Wright, Gavin Andresen, Shinichi Mochizuki, Dave Kleinman, Elon Musk, and many more…

…but also heard that Satoshi is the NSA, CIA, Mossad, KGB, US government, but if you follow along the chapters of this book, you probably know that Satoshi had to a Cypherpunk member. There is a long list of names on the Cypherpunk mailing list, but only a few, who was interested applying cryptography, on electronic cash. Those who came forward publically with a project, or design that is close to Bitcoin, are:

- Nick Szabo with Bit Gold
- Hal Finney with RPOW – known as Reusable proof of work
- Wei Day with B money
- Adam Back with Hashcash,

But they all denied to be Satoshi, in fact Hal Finney past away in 2014, so the great mystery of Satoshi continuous.

Chapter 9 The Distributed Ledger System

In the following chapter I will cover blockchain basics, including transaction overview, transaction fees, how new value enters the system. Also explain bitcoin mining, who are the bitcoin miners and what are their responsibilities, the process of bitcoin mining, block reward and block validation process, but let's start with the overview of distributed ledger system. When you think of a ledger system, there is nothing new about it, since every bank has their own private ledger. The key difference between a Bitcoin-blockchain ledger, and a typical private ledger, is that the blockchain ledger is publically available, anyone with internet access can view it, and this is because it's decentralized, instead of privately controlled. The Bitcoin Blockchain, also know as: the Ledger System, Distributed Ledger, Decentralized Distributed Ledger, or The Great Ledger. There are many different types of Blockchain exist today, however the Bitcoin-Blockchain was the first ever implemented, and the way is structured, is very similar to a Family Tree, but instead of names, it contains transactions and wallet addresses. One part of the Ledger contains the values assigned to the wallets, and another part of the ledger represents the date and time of each transactions. It's very similar to a bank system, but the great ledger has no banker. Every wallet address and the value they hold are visible to anyone publically, but only those can access each wallet that holds their private keys to those wallets. This is also why the system allows you to become your own bank.

Chapter 10 Transaction validation

In this lesson, I will talk about bitcoin transactions. Every bitcoin transaction ever made, is confirmed for its validity, and once validated, placed into a block. Each new blocks are also validated, then joined to the previously validated blocks, forming a chain of blocks, which is why we call it Blockchain, but Satoshi always referred to it as “proof of blocks”, or “chain of blocks”. Every node that is running the Bitcoin Core software, is required to keep a copy of the latest Blockchain, and Each block contains hundreds of transactions. This method ensures the rightfulness of every transaction, without having any central authority, or trusted third party. Before the system would accept a new block, every node must check the logical continuation of all values in the new block, and this is to ensure, that all transfers of costs are legit. This also prevents any replication of transfers, or any counterfeiting. It’s a crucial step, because this data will remain within The Great Ledger or Blockchain, forever. This process uses hashes of computation to validate each block, and make sure that each Bitcoin node receives the same record of the ledger. This process is repeating itself in about every 10 minutes, and each transaction once validated is sealed into the ledger. This is carried out by the miners, and it’s also known as Bitcoin mining. I will talk about bitcoin mining shortly, but before, I will explain how new bitcoins enter the system.

Chapter 11 Bitcoin mining fundamentals

In this chapter I will explain how new bitcoins enter the system. Once you install the Bitcoin Core software on your computer, it will begin to mine bitcoins, of course I don't recommend doing that if you have a personal computer, simply because mining bitcoins became very difficult and expensive. Bitcoin mining with personal computers would cause your CPU and GPU to be blown away. You would also get a huge electricity bill, and wouldn't have any bitcoins mined. To give you an idea what is to mine bitcoins with your personal computer with a very good gaming laptop, you could look at about 100 months by the time you could mine 1 bitcoin, which is about 8 years. Of course a super expensive laptop would became useless within a few months, and even if it would keep up the mining, after about 18 months the CPU, or GPU wouldn't be good enough anymore because the hashing difficulty on Bitcoin mining is increasing in about every 14 days. To be specific the difficult adjustment is changes in every 2016th block, and considering 1 block in about every 10 minutes, having around 144 blocks in every day, the difficulty increases, in about every 14 days. This is November 2020, and the price of Bitcoin mining is estimated between 5000 to 8000 dollars, including all electricity costs, paying for cooling systems and of course the mining rigs. The range is quite large, because it all depends on what country you mine, what equipment you use, is there a cheap or free electricity that you can utilize, and what kind of cooling system you have if you need any at all. For example if your mining operation is based in a cold country like ICELAND or FINLAND, your costs are considered a lot lower. So these mining rigs I am talking about are specialised ASIC hardware, created to do one thing, and one thing only: mining bitcoins. ASIC or esic, stands for Application Specific Integrated Circuit, these are specialized chips, customized to carry out specific task. Cisco switches are also using ASIC chips to carry out forwarding decisions in terms of switching, but in the case of Bitcoin miners, they carry out bitcoin mining only. The Bitcoin core software must be online in order to became part of the Bitcoin network. Once you are part of the Bitcoin network, the miners will start to mine bitcoins. Back in 2008, Satoshi has implemented the Blockchain in the way, so that the total supply will be 21 million bitcoins. Satoshi could have released all 21 million bitcoins in the first place, but the value of the coins would be

worthless, so he started with a moderate amount of bitcoin creation. Satoshi thought that once the Bitcoin community grows, more value creation will be required for the system to be kept secured. In order to keep the system maintained, Satoshi came up with the solution by creating a maintenance role, which solves two issues. One, is to ensure Permanently validating transactions, and the second is adding new value, into the existing system. The title of this role called “miner”, or “bitcoin miner” which used to be taken on a voluntary basis, but nowadays, it become a very profitable occupation. You might choose to mine by yourself, using your own hardware, but there are also mining pools, which you can join, and get a percentage of all the successfully mining blocks, or mining rewards. The analogy of mining or miners came from an idea of gold mining where Bitcoin miners, using computation power to create new bitcoins, similarly to gold miners, who mining underground, so they can bring new gold to the market. Bitcoin miners also have a responsibility of sealing each transactions into the ledger, and for this reason, we can also describe the miners, finalizers or authenticators. To get rewarded for such work, the miners receive bitcoins, and this is how new value is added to the system. The miners validate, authenticate, certify, and finalize the transactions by specific processes. Once the miners create a new block that is accepted by every Bitcoin member on the network, the record of the transaction cannot be modified, making it permanent information. This data, also becomes irreversible, so no one can ever challenge it, or change it in the future. Miners are sealing the blocks, which itself can take an enormous amount of computing power, ensuring that the process cannot be easily replicated. There are multiple methods that each miner may use for validating processes. For example, some of them might use different software, even creating their own in-house built software to speed up authentication processes, which you can do in linux, windows or Mac, but it doesn’t matter what software the miners use, because all of their work will be checked. Mining starts when the miner begins to gather transactions which are broadcasted on the network, and the miners receive bitcoins as a reward for each sealed block that’s added to the Blockchain.

Chapter 12 Block reward process

In this chapter, I am going to talk about the Bitcoin block reward process. When the Bitcoin system went live back in the 3th of January 2009, the reward for each block validation was 50 bitcoins. There are approximately 144 blocks becomes validated daily, so there is a new block being created in the system in about every ten minutes. In about every 4 years, the reward for block validation is halving. The first block reward halving taken place on the 28th of December 2012, when the reward has reduced to 25 bitcoins for each block validation. Next, the second halving took place on the 9th of July 2016, reducing the block reward to 12.5 bitcoins. The next algorithm change has taken place on the 11th of May 2020 when the reward for block validation dropped to 6.25 bitcoins. The next halving will take place around 2024. In case you wondering why there are no specific dates for the next halving, and why I say that new blocks are created in about every 10 minutes and not exactly in 10 minutes, the reason is simple. But first, let me ask you this: what happens when 2 different computers solving the same block in the same time right? Who gets the reward? Well, I just said it's simple and I will do my best to explain, so you understand. First of all, for two nodes or computers to succeed solving a block, the chances are very low, still it can happen, in fact it does happen every day, even happens multiple times per day. So, if two nodes might solve the same cryptographic puzzle in the same time, they actually both became winners, but none of them actually get rewarded. Instead, they both have to carry on doing a small competition between themselves, for solving the next block. Solving an even more difficult puzzle in the same time, the chances are becoming even lower, but if they both solve the puzzle in the same time again, the competition continuous, but, the difficulty also increases, and for the third time for both became winners, or solving the puzzle by the same time, the chances are even lower, in fact, is actually nearly impossible. Bitcoin transactions are immediate, yet Satoshi has defined it in the Bitcoin white paper; for transaction validations, nodes should wait 6 confirmations which is about 60 minutes. This is because the chances for two computers to win the block reward in the same time 6 times constantly, is completely impossible. So if you make a bitcoin transaction, which is immediate, but doesn't get validated within the next 10 minutes, your wallet would normally says it's

unconfirmed. Basically there is a competition running at the background between 2 or more computers. I also heard people telling saying that bank payments are faster, and it's also immediate, but it is not true. You might be able to see monies on your balance immediate, but confirmation on international transactions, or even transfers between different branded banks, can take 3-5 days, or even more. The banks have to settle between each other, the validation process can take easily a week, sometimes even 2 weeks. Bitcoin transactions in the other hand are always immediate, and the validation will be complete within 60 minutes for sure. Anyhow, back to the block reward process, the reward changes in every 210,000th successfully mined blocks, which is why there is no exact date. Instead, we say that in about every 4 years the block reward will be halved. This process will continue roughly by the year of 2140, until all 21 million bitcoins will be mined.

Chapter 13 Block Validation process

In this chapter, I will explain the block validation process, step-by-step in plain English.

Step 1. First step is to start a new block.

- Even if the miners are half-way done validating a block, if the block they are working on gets validated faster by another miner, they will drop the current process and begin concentrating on a new block.

Step 2. Next, they select a new transaction.

- This is when the miners choose, from hundreds, or thousands of transactions that are broadcasted over the network.

Step 3. Next, they check the priority of the transaction.

- This time, the miners can go back to step number one, and start a new block if they find the transaction they have selected previously is not that significant, but if the priority is high, the miners may go on, and move to the next step.

Step 4. Check if the transaction is valid.

- This is a process that every miner must check, there is no exception of avoiding this step for any miner, and if the transaction is found to be faked or invalid, the miners have to stop the process, and go back to step number 1, and start a new block, and find another, hopefully valid transaction.

Step 5.Next, miners have to accept the transaction.

- If the previous transaction was tested as a valid transaction, it must be accepted.

Step 6. Next step is to seal the transaction.

- Again, if the transaction has been found valid and accepted, now it's time to seal the transaction.

Step 7. Next, they must add the transaction to the transaction tree inside the block.

- This process can only be done, when all previous steps have been verified.

Step 8. Next, they have to check the size of the transactions.

- The miners need to check, if there are enough transactions within the transaction tree to seal the block. If there are not enough transactions yet, the miner won't be able to seal the block, until there are enough transactions, so the miners must go back to step number 2, and select a new transaction, again and again until there are enough transactions, for sealing the block.

Step 9. Next, they must check for interruptions.

- This is the process where the miner must ensure there are no other miners who have sealed the block in the meantime with the same transactions inside the block.

Step 10. Seal the block.

- Once there are enough transactions for sealing the block, the miners must seal the block.

Step 11. Finally, they must broadcast the block.

- The miners must broadcast the new block that's been sealed; but if the miners have been interrupted within the block sealing process, they have to start a new block all over again.

Step 12. Next, they must start a new block, but as you see, we are now back to the first step, as the process is repeating itself in about every 10 minutes.

- Miners could get interrupted while they are sealing the block, or broadcasting the sealed block, and if the block has been sealed by another miner, the block will not be accepted, therefore, the miner must start a new block. Fundamentally, the miners who successfully adding a new block to the existing chain, get rewarded 6.25 bitcoins.

Chapter 14 Transaction Fees

In this lesson, I am going to talk about transaction fees. I often hear the question: What will happen with the miner roles once they don't get any block reward? First of all, once all bitcoins are mined, the inflation of Bitcoin will go to zero, and the miners will obtain income from transaction fees, which will provide a motivation to keep mining and keep transactions irreversible. Transaction fees are included when you make a transfer, so the transaction will be processed by a miner. The current block size is now 2MB , and each transaction is a size of between 150 to 500 bytes. The transaction fees are calculated, according to the size of the transaction, and not the amount of bitcoins being sent over the network. Once the block reward reduces over the time, it will be replaced by transaction fees, but there are second layer technologies, such as lightning network that is already reduces transaction fees dramatically, which are extremely useful for micropayments. I also mention that once you make a bitcoin transaction, in most wallets you have an option to make it a priority transaction, which will cost you more than a regular transaction. For example if you make a transaction of a small amount like point 1 bitcoins, you most probably will keep it as a regular transaction. But if you about to buy a Lambo or Tesla, you would probably make sure that the transaction is more secured by the miners, and processed as a high priority right? If you think in terms of fiat currency, for example when making a transaction of 10 dollars to buy a book, is not such a big deal, but if I would transfer 10,000 dollars to my father, I would be happy to pay 10 dollars to make it more secured, even 100 dollars if that would guarantee the founds to be transferred securely, especially if the money is urgently required. So my point is that there will be always people happy to pay extra fees, to ensure transactions are sent with high priority, and for this reason transaction fees will disappear ever. This is very good for Bitcoin, as there are more Bitcoin nodes participating, sealing transactions, more secured, and more decentralized the network become.

Chapter 15 Supply and demand

There are many factors that could move the price of Bitcoin, but its all about supply and demand. When it comes to the supply of Bitcoin, is basically given, which is 21 million bitcoins. This is also known as controlled supply, so there is no quantitative easing, no new money injected into the market randomly, instead we know exactly that in every 10 minutes there are new bitcoins, which are halved in every 4 years. It is estimated that over 3 million pre mined bitcoins are lost in space, as many people have lost their private keys to their bitcoins, which reduces the total of 21 million units to around 18 million that will ever be in circulation. Also Satoshi has about 1 million bitcoins, which he never touched, and probably never will, so it really comes down to about 17 million bitcoins. When it comes to the Demand: There is a tremendous amount of demand, which continuously increasing, making the value of Bitcoin even higher. When I say that, I don't mean from one day to another, but overall year by year, the price of bitcoin is continuously growing. Moreover, the supply is continuously decreasing in every four years, which also makes the value of Bitcoin even higher. This is because In every four years, the block reward is halving, so less and less bitcoins will be mined, while the difficulty to mine those coins are continuously increasing, which also means, that the cost of mining will increase, and that will also increase the price of Bitcoin. To learn more about the difficulty increase of the Bitcoin blockchain, visit the following link;

https://blockchain.info/charts/difficulty

Another economy effect is that while the value of Bitcoin will rise, the value of Fiat currencies will decrease, which makes the value of Bitcoin even more higher. I have been predicting the price of Bitcoin multiple times, and often I was right, but not always, so I just try not to say the exact amount and how much it can became within 5 or 10 years because I might be completely wrong. Anyhow, there are few facts that logically indicate a continuous grow of the future price of Bitcoin, but as I said earlier, it all comes down to supply and demand.

Chapter 16 Network Effects & BTM-s

In this chapter I will talk about the network effects of Bitcoin. So, Everyone talks about Bitcoin, maybe not all the time, but there is a continuous increase in term of people want to know more. For example, those who used to hate it for reason like it was used on the dark web, now looking to invest in Bitcoin, or at least considering a possibility of it. Those people who were sceptical, because continuously making new headlines in the media, they are now learning about it. Another key point is that Bitcoin is legalized everywhere, which makes it even easier to people to participate. By the way, back to the dark web example, Bitcoin had a bad name for years, because it was used as a payment method to buy drugs. Still, according to statistics, the largest payment instrument for paying illegal activities, are still fiat currencies such as the dollar. Also, I personally don't see any point of buying drugs with bitcoin, I mean why would an average person would pay for such thing online, if you can just go to the street and buy there right? Bitcoin is semi anonymous, and the transactions will be always traceable on the blockchain, but in the other hand, withdrawing 20 dollars from a traditional cash point and spending that for drugs that's so much easier. The problem seemed to be a misbelieve amongst criminals, and drug users, that Bitcoin is completely anonymous, which is not correct, but they were using it anyways. The payment instrument used by criminals should not be judged, instead those who have with bad intentions. Criminals also use internet, cars, cell phones, microwaves, but in terms of money, they also use dollars, and swift wire transfers, but normal people with no criminal intension also using the same technologies and monies right? So it's not the technology, or money that should be blamed. Bitcoin had a bad name for years, but this is now changing, as more and more people understand it. That was all about the media paining a dab picture on bitcoin. Media always love to use dramatic headlines, so they get more attention. In terms of network effects, back in January 2018 there was about 2000 Bitcoin ATM-s in 61 countries, and by November 2020, the figure increased to 11816 Bitcoin ATM-s in 70 countries around the world. BTW BTM-s are short for Bitcoin ATM-s. To learn more about where are the nearest BTM-s to you , visit the following page:

https://coinatmradar.com/

Online Markets like cryptocurrency exchanges, are also in the rise. In 2018 we had 7800 Cryptocurrency trading exchanges, but as of November 2020, there are 32631 platforms around the world. There is a lot more I could talk about demand, and what network effects the Bitcoin market creates, but I believe I mentioned few that provides enough reasons to prove the point in relation to huge demand.

https://coinmarketcap.com/all/views/all/

Additionally, if you want to see and compare all the markets exist today, visit the following page:

https://coinmarketcap.com/currencies/bitcoin/markets/

Once on the site, you will be able to compare the prices of Bitcoin on all markets against both Fiat and crypto-currencies.

Chapter 17 Market Manipulation & Price Predictions

In this chapter, I will talk about market manipulation and how it can effect the price of Bitcoin. In terms of manipulating the price of Bitcoin, I think there was always a case, but when it became intentionally recognised, it really began in 2017, when we all witnessed a bull market. China News was dominating every news channel and papers all the time. Most of the Bitcoin mining is in China, because of cheap electricity costs, so mining bitcoins in China, is the most profitable. Within less than a year many Chinese miners have moved their operation to other counties. Started with China announcing that they will probably ban cryptocurrencies, followed by a drop of crypto prices. Next, they have announced they only been thinking about banning, then the prices gone back up, but a week later, they announced that they are thinking about banning Bitcoin, so prices went back down again. Two weeks after that, they said they will not ban Bitcoin, and the prices soared again. So this was the game they were playing for a while. In fact the Chinese government played it very well in the end, as they managed to ban most of the exchanges. ICO-s known as initial coin offerings, which is very good in my opinion because most of them was a scam, and they also managed to ban most of the Bitcoin mining farms. As a result, the Chinese government has managed to overtake and run only a few exchanges, and a few mining farms. What also happened, is that those Chinese people who were heavily involved in mining, or running online exchanges, simply moved out from China. Today, they are all over the world, places like Malta, where they pay even less tax, or Canada and Iceland where they don't have to worry about cheap electricity for mining anymore. They can save even more money than before, either because less taxes needs to be paid, or less money need to be spent on mining, because mostly these countries are always cold and no cooling systems required. Anyhow, it's a long time I have not heard of anything from China in relation to crypto, and it would be probably irrelevant anyways. Because with these manipulations, all they achieved is to decentralise the Bitcoin network even more. They wanted to take full control of the Bitcoin network, but instead, they decentralized it even more. As you see, before all these announcements, threats, banning ideas, it was estimated that 70 to 85% of all Bitcoin mining was in China, but now is reduced to about 55-70%. Chinese news announcements have taken a huge impact on the price of

Bitcoin. For example, when China has announced that they are re-opening all Bitcoin exchanges, just a month after they have closed them, the value of Bitcoin has risen from $6000 to $7800. Because of these tremendous volatility in price, the figures have reached what we have never experienced with any other currency, and Bitcoin has become a paradise for traders! Many people left behind traditional trading with fiat currencies or precious metals, to learn and invest in cryptocurrencies instead. Risk Analysts, technical analysts, time analysts, money managers, hedge funds, and other financial organisations, not only started investing and trading with Bitcoin, but also advising their customers, where they should keep their money. In 2017, traditional money managers would tell you to keep your money in bitcoin, but in 2018-2019 we have experienced a bear market, so there are also some new games, that we can witness, all over the news. I try to keep names out of this, but there are more and more hedge funds, and money managers come up with all sorts of predictions, on the price of Bitcoin. For example they would go and make announcements that the prices of Bitcoin will hit 100,000 dollars by end of 2021, and it will be 500,000 by 2022. So, they would try to convince a large part of the population to buy in right? They don't say, go and buy, they just predict. So what happens is, that lots of people think that these hedge fund managers must know something, and when people begin to buy bitcoins the prices would rise, which creates a network effect to buy, and prices would go up for a while, maybe for few days or even a week, and then a week later the price would suddenly drop right? So the game they play is simple, they convince the world to buy, without saying it of course, which creates higher prices, then they sell, once the price is high enough for them. What they don't tell you in their public announcement ,is that they are responsible of other people's money, and many have invested in Bitcoin when the price was higher than today, and suddenly they want their money back because it's a bear market in Bitcoin, and maybe they found a better short term investment, maybe they can't wait any longer, maybe they just running out patience or money or both. So before they would sell, they ensure to get a better price by manipulating the price, and because they cannot buy obviously, they would make unqualified investors to buy for them. Pumping the price, so they can get out on the top. People with good connections, having 5 minutes interview on a well-known news channel, they can be pretty convincing, so look out for bold announcements like that. I have been learning from some of the best technical

traders, and they all would agree that people announcing the price of Bitcoin for longer than the next few days, these people either have no clue what they talking about, or want to achieve something by saying that. Of course they would always deny any sort of market manipulation, and they never told anyone to buy anyways, all they do is predict prices right? There are many sorts of market manipulations out there, but this prediction type, seem to be very popular recently, so if you are a trader, or want to become a trader, you should look out for announcements like that, as it could lead you to bull trap. Bull traps are called bull traps for reason, and it’s because is a trap for bulls!

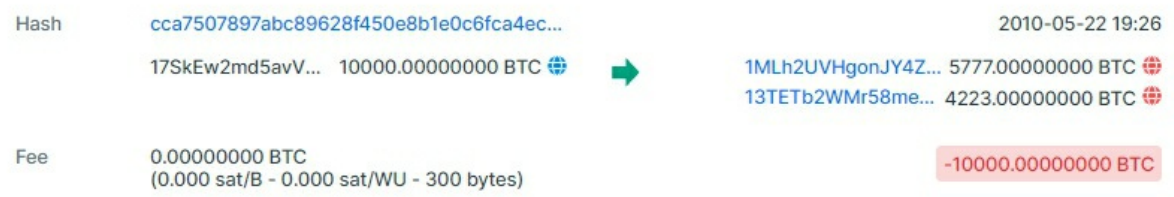
Chapter 18 The best time to buy bitcoins!

You must have heard people saying: “It’s too late to buy bitcoins!’’ Or, “It’s too expensive already!’’ And the fact is that it’s true, it doesn’t seem to get any cheaper in terms of dollar price, but there is a reason why it’s value continuously accelerating right? For example, when first time I heard about Bitcoin it was 300 dollars, and I thought to myself: How on earth this bitcoin can worth 300 dollars, I just couldn’t believe it. At the time I had no clue what Bitcoin was and if I had to guess, I imagined that is a physical token of some sort. I didn’t do any research at the time, but next time I heard of Bitcoin about 2 years later when Wannarcy ransomware was all over the news, the price of Bitcoin was about 1700 dollars. In case is first time you hear about WannaCry, it was a cyber-attack, lasted 4 days back in May 2017, targeting computers running Microsoft windows operating systems, which eventually hit about 300,000 computers in more than 150 countries. The computers became unusable, and files were inaccessible, while the Cyber gang or hackers, asked for a ransom paid in bitcoin, for unlocking computers, so they can be usable again. Back to the Bitcoin price, I just couldn’t believe that is gone up again so much! I thought 300 dollars was already too much, but 1700, is definitely over the board. At this point I still didn’t buy any, but began to study and learn as much as possible about the technology by reading books, blogs, forum posts, watching video courses, presentations and documentaries. By the time I was confirmable to start investing, the price of Bitcoin was already 2400 dollars. In the other hand, you hear people they bought bitcoins in the early days like back in 2010, invested 20,000 dollars, when the price of a coin was about 20 cents, and they are now Bitcoin millionaire right? Well, I am not a Bitcoin millionaire, and being honest, those people had a nerve to do such thing, because they clearly didn’t understand much about Bitcoin, unless they were developers, or have close connections to Bitcoin Devs. But the fact is that Bitcoin had major bugs through years up until 2014, and the network was instable, and once the bugs were fixed and Bitcoin adoption began to rise, there was a scalability issue, as the adoption rate was too high for the network, which only got resolved in 2017 by implementing Segwit, known as segregated witness. Basically, if you started investing in the early days, when there was low adoption, no wallets, no merchants, various technical issues, like unstable network and

major bugs, investing in Bitcoin was more like a gamble, or a long term bet. You might have heard about the Bitcoin pizza guy, or the story if the most expensive pizza? If you not familiar with the story, basically a Bitcoin programmer, named Laszlo Hanyecz, in May 2010, posted a request that he would like to buy pizza, and wants to pay with bitcoins. Eventually he managed to buy 2 pizzas for 10,000 bitcoins, which was the first recorded Bitcoin payment that was in exchange for goods. This is a very famous story ever since, and people quote all sort of figures that it was a 15 million, or 85 million dollars' worth of pizza, and some people also says that he was stupid to spend 10,000 bitcoins on 2 pizzas. The reality is that the coins were nearly worthless at the time, didn't worth not even a penny, so Laszlo said that he made a really good deal at the time, and he had no clue that the price would ever go up in value. If you want to look at the transaction where Laszlo spent 10.000 BTC-s for 2 pizzas on the 22nd of May 2010, visit the following link;

https://www.blockchain.com/btc/address/17SkEw2md5avVNyYgj6RiXuQKNwkXaxFyQ

In BTC:



In Dollar value as of November 2020:



At the time they said that those 10000 bitcoins were worth about 41 dollars, and eventually the pizza merchant also sold his 10,000 bitcoins for 400 dollars, making 10x on his money. Yet, today those 10,000 bitcons worth $159,420,500. With these stories, I just want you to see that investing in Bitcoin never seem too late, and most people say that the best time to buy bitcoins is yesterday, but my advice is that you should only buy bitcoins once you feel comfortable doing so, and don't let the price bother you, because in

long term, the value will be increasing anyways. By the way, if you want to became a millionaire overnight, Bitcoin is not for you. Bitcoin, as an investment will appreciate its value, but in the long term and not overnight.

Chapter 19 The worse time to buy bitcoins!

In this video I will talk about when is the worse time to buy bitcoins. The actual answer is not exactly a date, but a human behaviour, which is called FOMO! Fomo stands for Fear of missing out, and before you think it's such a nonsense, let me tell you, that FOMO is very powerful, and it can move the market tremendously. Fomo can infect a wild range of people, including unqualified investors to experienced traders, even technical analysts, money managers, but even large hedge funds. You see, FOMO is still underestimated by most people, even they know it exist, and they know they wouldn't get caught of it, but eventually we all experience FOMO. My experience with FOMO, is when the price of Bitcoin dropped from 17K to 11K, I quickly logged on to blockchain.info to buy bitcoins, but most exchanges couldn't coop with the demand, so I couldn't buy, and the situation was very frustrating. I really felt like I am missing out on a cheap price, and I did, because 4 hours later, once I was able to logon to the exchange the price has increased to 14K, and guess what!? I still bought bitcoins even for that price, because I was in such a hype to buy bitcoins, I just couldn't wait any longer. And of course the following day, the price went back to 11K again. After that event, we had a bear market for over 2 years where prices were stuck between 6 to 8K. That was the first time I experienced FOMO, and hopefully the last as well. You see the prices were even 20K already, and many people speculate that was illegal trading, or cartels manipulated the market, or it was pumped by whales, because of the Bitcoin futures market, but what really happened on the market is FOMO. Fear of missing out, created a bull run since the price of Bitcoin reached about 7K, and managed to triple of its value. Not for long of course, and that is because it was a HUGE FOMO on the crypto market. The problem is that most people in FOMO has no clue about Bitcoin, never watched a course, neither read a book about it, instead, heard in the news that Wall Street is about to enter the game. Especially after CME, and CBOE listing Bitcoin on the futures market, made everyone to run to buy bitcoins, and we mostly talking about unqualified investors, having no investment advisors or money managers beside them. In the other hand, those who knew that the market is going through some crazy hype, and Bitcoin is overpriced, started selling and made a large profit. In the meanwhile, those who got involved when the price

was about 15-18k, realised that is now back to 12K, started panic selling, which pulled the price of even lower back to 10K, then further down to 8K, which was a reasonable price even before the FOMO hit the market. So the problem with people when it comes to FOMO, is that they all say things like:

“Ahh yeah, I wish I would have bought bitcoins when it was 10K, but when it goes back to 9K, instead of buying more, they panic sell, because they now fear that the price will go even lower.”

So, my advice is that if you feel like you are experiencing FOMO, you should stay away from buying. Don’t buy because of FOMO, it can and it will hurt you, both: emotionally, and financially.

Chapter 20 Button line on buying bitcoins

In this chapter I would like to express my final thoughts, and advise on buying bitcoins. This is not a financial advise of course, only my honest opinions. So you take it or leave it, or better; learn from it. I have talked about FOMO, market manipulation, hype, crazy news announcements, price predictions, investors, traders, Bitcoin futures, network effects, supply and demand, technical issues, such as scalability issues, so there some good, some bad, some thinks are certain, some are not. So, I really want to emphasise that if you are new to Bitcoin, don't just go and buy in a "fomo" state because there is a crazy news announcement. Instead, educate yourself and only buy once you are comfortable doing so. Others might advise you differently, like;

"Go buy now! You will learn about Bitcoin later" It's too late already!"

But I personally find it wrong to invest in anything that you haven't done efficient research about, and then worry or speculate what might happen, and waiting for the next news announcement. I think it's wrong. But, if you don't want to learn about Bitcoin, you are not interested in studying it, or you don't feel like you have a technical expertise to understand, or even if you don't have time, maybe because you are working too much, or your family takes away all your time, or anything like that, but you still want to invest, you should consider hiring a Bitcoin broker, or money manager. Someone you trust, or you know someone who trusts him or her using his services. Hiring an advisor offline, or even online is not wrong. You don't have to know everything, so you can outsource it anytime, anywhere on the world you leave in. My next advise in terms of how much should you invest is that you should not invest more then what you not afraid to lose. Some people defines it as 5% or 10% of their portfolio, but some people just have some saved stash, which maybe 70-80% of their portfolio, and they want it all in. If that's what you want to do, because you confortable of doing so, it's all up to you. My final advice in terms of percentage of investment is to try breaking down your investment. For example, if you have 1000 dollars to invest in Bitcoin, don't do it at one time, instead buy for 200 dollars on the 1st of the month, then buy 200 dollars' worth a week later or even 10 days later. Then 200 dollars' worth a week after again, and so on. This would help you practice making purchases, and also would create an average investment price.

So for example if the first time you buy when the Bitcoin price is 10K, but the second time you buy is 6K, your average of investment is about 8K. I hope you follow along. So if you would invest all your money at the first time, when the price is 10K, that would be your average. Investing in multiple occasions can be useful because there are days, when price volatility of the Bitcoin can be 10, even 20%.

Chapter 21 Why would you use Bitcoin?

In this chapter, I will simplify why Bitcoin is so powerful. First and foremost, it solves several issues:

- You don't need a bank, and anyone can have a wallet for free.
- You can send bitcoins to any individual in the world, at any time, costs only a little fee and you don't have to involve any third party.
- People in underdeveloped countries can easily access it, because all its required is Internet access.
- No central governance, therefore, no authority can control your money.
- Bitcoin is optional: basically nobody forces you to have bitcoins.
- No single point of failure, because it's a peer-to-peer decentralized network.
- No Inflation. Basically there is no continuous injection of bitcoins into the marketplace, no QE, because it has a fixed supply of 21 million bitcoins.
- Growing demand: while there is a rise in demand, the value of Bitcoin will continuously increase.
- Bitcoin is legalized. There are more and more countries where Bitcoin is already legalized and accepted as a payment method.
- Bitcoin is trusted by its adoption. Bitcoin has a Decentralized ledger system: Bitcoin is using a chain of blocks technology, known as proof of work or Blockchain, which become very famous in the recent years for its security and it's trustworthy, even heard people calling it: The Trust machine!
- The systems saves manpower: Bitcoin doesn't require human administrator in order to validate transactions.

There are many more properties I could talk about, but I wanted to provide the main reasons why you can start using Bitcoin in your everyday life.

Chapter 22 Bitcoin is dead

You might come across of the sentence or announcement: Bitcoin is dead right? Bitcoin has managed to die 383 times already.



Source: https://99bitcoins.com/bitcoin-obituaries/

Basically when Bitcoin makes it to the news, its repeatedly connected with some negativity, and Bitcoin was the most famous for being a currency of the criminals and things like that. Well, Bitcoin payments can be transferred all over the world with anonymity if chosen, so criminals still use Bitcoin, but they also use dollars, euros, pounds, and all sorts of other monies too.

Unfortunately, Bitcoin has been introduced with a bad reputation in the past, and it seems to continue by the media who love to create a juicy headline. Another situation when people calling Bitcoin dead, is when Bitcoin hits a milestone in value. Bitcoin was dead when it reached $100, then died again when it hit $200, then again when it hit $1000, then it died again when it hit 10000 dollars, even in December 2017, when Bitcoin hit 20000 dollars, it has died once again. There is a website which collects all articles in relation to the death of Bitcoin, called 99bitcoins.com. This site is a collection of all those stories where Bitcoin was in the news as a dead currency for all sorts of reasons. The first time Bitcoin went dead in December 2010. Since that painful event, Bitcoin has died more than 300 times, yet still, exists. What we can learn from this, is that more often Bitcoin dies, the more it will hit the news, so more people will hear those fake news stories when Bitcoin has died. This also provides many opportunities to people for additional research, and decide for themselves if Bitcoin is really a dying cryptocurrency, or not. Imagine that you heard back in 2010 that Bitcoin is dead, then you read another article in 2011 where Bitcoin is dead again, and hear this all over again and again for 10 years now. So, obviously something isn't right. So it seems, Bitcoin will carry on ending up dead, again and again, (at least in the news), but the fact is that Bitcoin is here to stay!

Chapter 23 Bitcoin is a scam

OK, Bitcoin is obviously not a scam! Many people used to claim that Bitcoin is a scam, but this is not so much the case anymore. What you must look out is ICO-s, initial coin offerings, so called new and better cryptocurrencies that will take over the world. Those are dangerous and pretty much 95% of all ICO-s, alt coins, alternative coins are actually a scam. Most of them exist to scam people, these are basically Bitcoin clones, and there are many many out there, so you really need to look out, making sure you have nothing to do with them. But there are a handful of cryptocurrencies, which was fairly mined, no ICO or money collection was involved, but most of them having no use cases at all, but basically not all Altcoins are scams just most of them. Another think I want to mention in relation to this topic, is that if you go ahead and buy Bitcoin from someone who scams you. That's a different story, and if that happens, the person is a scammer, yes, but Bitcoin is not a scam. People who says that Bitcoin is a scam, they most probably don't know the meaning of scam. What you should know is that there are Bitcoin related scams all over the internet, and scammers claim all sort of thinks like doubling your money if you invest 10 bitcoins, or you get daily profit and thinks like that. But, let's understand exactly what a scam is. First of all, a scam requires hidden information, but Bitcoin is an open source Protocol. Bitcoin is a very complex technology, but, still anyone can download it and take a look at its code, so there is no hidden information. Bitcoin is using Elliptic Curve Cryptography to participate in a discrete logarithm problem, also uses SHA-256 hashing algorithm, as well ASCII encoding, and many more technologies combined. The fact is that most people who calls Bitcoin a scam didn't bother to learn about it, especially didn't bother to understand the technologies, which upon Bitcoin was built on, instead just call it a scam. If you want to learn more about these technologies, you should check out my other book called "Bitcoin is blockchain, and here is why!" In summary, I just wanted to clarify that Bitcoin is not a scam.

Chapter 24 Bitcoin is a bubble

In this chapter, I will explain why people call bitcoin a bubble. First and foremost, it is very difficult to say, because times have changed, and we are entering a digital age. In the Digital Age everything changes rapidly, so we must educate ourselves with the new rules of the game. Bitcoin represents FREEDOM from FIAT currencies, which are the very cause of financial bubbles. I have talked about quantitive easing before which explains some of these issues. Bitcoin is NOT a financial bubble; instead Bitcoin is a new digital currency with no borders. People refer to it as a bubble, as they only can compare to other bubbles like the tulip bubble, or housing bubble, or even the dotcom bubble. We really shouldn't compare Bitcoin to any of these bubbles, as we have never experienced anything like this, but the closest we could compare Bitcoin is the dotcom bubble. Being more specific, if I have to compare something to dotcom bubble, I would say that we have a cryptocurrency bubble, or ICO bubble, instead of Bitcoin bubble. Back in the dotcom bubble there were hundreds of technology companies, and each of them were getting founded with crazy amount of money, but 10 years later there are only few companies left and the rest of them have disappeared. Back in a Dotcom bubble, if a company announced publically they have a website and selling movies on demand like Enron did, suddenly their stock gone through the roof and the company just became 100 million dollars' worth more. While in the back ground, they had no movies to provide streaming, no technology was existed to accommodate these functions; all they had is an announcement. And this is exactly what happened with the cryptocurrencies and new ICO-s as well in 2017. Every new ICO that announced something fancy, like its faster than Bitcoin, more secured, or more anonymous, all started pumping, while there was no product, only promises. I have seen many of these companies coming up onto top 10 cryptocurrencies in terms of market capitalisation, and suddenly, once they could scam people anymore, they completely disappeared. Some of these major scams and ponies finally gone busted like: bitconnect, onecoin, secretion, litecoin red, high reward, or parodies like jesuscoin, bitcorn, true coin, Saladin coin, and so on. As you see it seems like we are in a cryptocurrency bubble right now, but Bitcoin is something else.

Chapter 25 Bitcoin is a stock

In this short lesson I will clarify that Bitcoin is not a stock. First of all, stocks are equity positions in companies. For example you might own a percentage of Amazon, Facebook, or Apple, but when you own bitcoins, you own an asset which is limited in its circulation due to its controlled supply. The possible misconception is understandable, as Bitcoin has some similarities to stocks, because there are many online exchanges where you can use Bitcoin for trading purposes. In terms of CME and CBOE listing Bitcoin futures, that not much to do with bitcoins, as you can bet on the bitcoins future price. If you participate, you are gambling. You can place bets in Fiat currencies, like dollars, so you don't need any bitcoins. BTW, if you bet and win, you get paid in dollars as well, not in bitcoins. So you won't have to buy bitcoins to participate in Bitcoin futures market. Neither will you lose or win bitcoins, because you will not get any bitcoins. So once again, Bitcoin is not a stock.

Chapter 26 Bitcoin is a pyramid scheme

In this chapter, I will clarify why Bitcoin is not a pyramid scheme. Lets' begin by saying that Bitcoin has no pyramid structure to talk about. The misconception is possible coming from the gains of Bitcoin in terms of fiat value. Bitcoin continuous increase in it's value, is coming from the limited supply of the coins. Basically more people buying the coins, the more valuable each coin becomes because the supply gets scarcer. But a pyramid scheme pays out dividend or commission, to seduce more people to join, whereas Bitcoin as an investment does not pay out dividend. Instead the return is coming from its capital gain. A pyramid scheme has no real business value, whereas you can buy goods or services with bitcoins. A pyramid scheme is a centralized system, with the con artists pulling the strings, collecting payments, and paying out dividends. Also, In a typical pyramid scheme the con artist can collapse the scheme anytime, by running away with the money. In the other hand Bitcoin is a decentralized system, and the inventor and early adopters of Bitcoin are unable to collapse the system even if they wish to do so. Satoshi designed, implemented, and published the Bitcoin software, but 80% of the legacy code has been re-written, and modified by hundreds of Bitcoin developers. So once again, Bitcoin is not a pyramid scheme.

Chapter 27 Bitcoin Skills Described

Bitcoin is a medium of Exchange

- In this chapter, I will explain why Bitcoin has a perfect use case to be a medium of exchange. The main criteria for something to function as a medium of exchange is that it has to be robust and portable. Since Bitcoin is digital, it obviously fulfil these functions. Bitcoin has all the properties, and beyond to be used as money.

Bitcoin is Censorship resistant.

- Basically, nobody can block or intercept a transfer of any amount, at any time. This fact brings me to the next point, that bitcoin is permissionless. The Bitcoin software can be installed by anybody, and used to send or receive bitcoins.

Un-freezable

- Basically nobody can freeze or seize your accounts.

Irreversible

- Once a bitcoin transaction is confirmed, nobody can undo it, like traditional credit card systems, such as refunds.

ID-less

- Basically it does not require ID or registration to use ibitcoins. So it can be used by people, computers, unbanked people, or even stateless people.

Borderless

- Basically it Works anywhere where there is internet.

Semy Anonymous

- While it can be used anonymously, most people don’t use it that way, but there is an option for it.

Accountable

- Sharing your public keys would reveal all your previous transactions, and anybody with those keys can see all your bitcoin transfers on the blockchain.

Great uptime

- The system Works 24 hours a day, 365 days per year, so it’s not like banks the might be close overnight, or the weekends.

Quick setup

- You can start accepting bitcoins very quickly, without setting up merchant accounts.

Push system

- Other internet medium of exchanges like credit cards are 'pull systems', where the receiver is given the sender's credentials, and then they pull money into their account.

Programmable

- A web server can understand or create transactions automatically, for example to release escrow, or automatically provide goods or a service. Also Smart Contracts can be written with a knowledge that will be followed no matter what. But, smart contracts were happening on Bitcoin first time, but the Devs have turned them off because they were buggy, unstable, and pretty useless. Other fancy

functions like multisignature or timelock allows Bitcoin to do things which other medium of exchange cannot.

Bitcoin is also fast

- Transactions are broadcasted through the peer-to-peer network in seconds, and they can become irreversible within an hour, after about 6 additional transaction confirmation. Bitcoin also can serve a purpose as a store of value.

Bitcoin is: portable, durable, recognizable, fungible, scarce, and hard to counterfeit, and its supply is guaranteed to be stable. As you see, Bitcoin not only a medium of exchange, but also can become a store of value.

BOOK 3

MEET THE ARCHITECT OF BITCOIN AND BLOCKCHAIN: SATOSHI NAKAMOTO

THE ADVENTURES OF THE CYPHERPUNK BILLIONAIRE CRYPTOREBEL

BORIS WEISER

Chapter 1 Early timeline from Public Evidences

In this chapter I will focus on the public evidences found in relation to Satoshi. When it comes to Satoshi's timeline, the actual interaction with people that he made only lasted about 2 years. Through those 2 years, nobody has ever met him personally, neither talking to him over the phone, or skype or any other type of voice call. Satoshi was only talking to people through forum posts and e-mails, but there are evidences that Satoshi was already active on the web before he would interact with anybody. The first evidence found is the bitcoin.org webpage registry. Satoshi has registered the domain, called bitcoin.org on the 18th of August 2008. The website; bitcoin.org is still up and running today after a decade past, and that's the very same website where you can also download the Bitcoin core client if you want to run your own full node. Moving on to the next public event, which was the publication on the Bitcoin whitepaper, called: "Bitcoin: A Peer-to-Peer Electronic Cash System." The whitepaper was published on a cryptography mailing list, but it was also available to download on bitcoin.org. Even nowadays, if you go to the website: bitcoin.org/bitcoin.pdf, you are still able to access the whitepaper. The whitepaper defines what is Bitcoin, how it works, and it contains about 8 pages, and an extra page at the bottom which lists the references related to the Bitcoin project. The whitepaper also has Satoshi's name on it, which indicates that he is a Japanese male but the e-mail address he uses is German, which can be found on the top of the paper as satoshin@gmx.com . The next event on our timeline is the 3rd of January 2009, when Satoshi has mined block number zero, also known as the Genesis block, which had a reward of 50 bitcoins. I will talk about the Genesis block later, and why it's important, but now I will move on to the next event on the timeline, which is the 9th of January 2009, when the first version of Bitcoin software was released publically, known as v0.1, pronounced as version 0.1. As of today, the beginning of November 2020, the latest version of the Bitcoin Core software is version 0.20.1, which was released on the 1st of August 20202. Moving on, the next famous event on our timeline is the 12th of January 2009, which is the first ever made Bitcoin transaction. Satoshi has sent 50 bitcoins to Hal Finney who was an excellent coder and a well known cryptography expert. Unfortunately Hal Finney has died back in 2014, though; his story not yet ends, but in this chapter only focuses on some of the

early notable timelines.

Chapter 2 Writing style of Satoshi

This chapter will focus on the writing style of the Bitcoin creator. Satoshi has been posting on a small number of forums, and sent plenty of e-mails to multiple people, but to be more precise, there are close to 100,000 worlds can be found publically that's been written by Satoshi publically. That's a lot of worlds and sentences, which can help us to spot a few trends in his writing styles, and one of the most helpful is that he was using British expressions such as ''bloody hard'' or ''bloody difficult''. Expressions like these, could be used by Australian too, but when it comes to his spelling style, it wasn't only British, as some of the words and sentences he used an American style, but not always. Another notable old fashioned writing style has been identified, which is that he always used double spacing after a full stop, which would indicate that he used to write with a type writer so most likely he stack with that habit. Other then that, Satoshi's writing style seems to be very well structured, and there are almost no typos or spelling mistakes. Moreover, he doesn't seem to reference anything from his personal lifestyle or relatives, hobby, as all his e-mails and forum posts are focusing around Bitcoin and how to make it more scalable or more user friendly. When people asking him about any personal inquiry, he always seem to be ignoring those, and avoiding replying to them. Satoshi has a scientific writing style, which requires a firm foundation of English sentence construction and usage. Because he has mostly used technical writings, he was able to pull only a similar sort of audience as himself, which didn't leave any room for an average small talk or chit-chat. Lastly, because the Bitcoin whitepaper was written in English and there was no Japanese version found ever, and of course he was always posting and e-mailing in English language, we should conclude that is not Japanese.

Chapter 3 Satoshi's Cryptography Skillsets

First of all, Satoshi was a PC user. Maybe it's nothing, but after researching on statistics on the differences between pc and mac users, there are some differences that might worth mentioning. The statistics referenced here was carried out by Hunch.com where they asked all their users to answer whenever they want for the following question: Are you a PC person or a MAC person? Close to 400 thousand people answered and 53 % of them replied that they are PC users, and only 25% of them are mac users. Once again, this might be not a big deal, but we have to remember that Satoshi was using a PC when created Bitcoin, and he really needed lots of help from others to make Bitcoin compatible with MAC and Linux. Moving on, to create Bitcoin, there are few fields that you should be familiar, and it is fair to say that Satoshi was an expert in quite a few field, other then coding only, so lets take a look at some of them. Satoshi has not only designed but also implemented the Bitcoin blockchain, so he had to be an expert on Economics, monetary history, peer-to-peer and distributed computing, databases, C++ coding and of course Cryptography. According to expert coders, they have analysed some of the early codes that Satoshi has written, and came to the conclusion, that he wasn't the best programmer, but a good C++ programmer. The Current Bitcoin blockchain developers confirmed that 80% of the early Bitcoin code has been modified, re-written since it's inception, and this is not because it wasn't written well, is just the Bitcoin network has been grown, and scalability always requires additional features and integrations, such as exchanges, payment networks, multiple types and brands of wallets, and so on which didn't exist back in the day, when Satoshi was still active. The final word is that Satoshi in his time was an excellent C++ programmer. One of the most important skillset of Satoshi, was really resided in Cryptography. I have also done research on cryptography experts, such as Bruce Schneier, Diffie and Hellman, Hal Finney, Nick Szabo, and few others, and they all seem to have something in common, which is to invent their own cryptography, but Satoshi has not invented anything new. Instead, he used existing cryptography that was already proven working, and build Bitcoin on the top of that. In the other hand, people said that he was always in the rush, but I personally don't think that he was looking for a shortcut, or anything like that, instead he wanted to avoid failure, and wanted

to have less room for thinks that could go wrong. I mean, why to take the risk, inventing something new, if there was already existing and working solution for his requirements right? Satoshi used E.C.D.S.A., also known as Elliptic Curve Cryptography, or Elliptic Curve Digital Signature Algorithm. Elliptic Curve Cryptography was first suggested in 1985, still, only been used wildly in 2004, and 2005. E.C.D.S.A. also uses traditional DSA, stands for Digital Signature Algorithm, which was first proposed in 1991 and the first version was released in 1996.

Chapter 4 Satoshi's Written Communication Skills

In this chapter I am going to carry on talking about some other skillset of Satoshi, which is humility. Satoshi has never seemed to be proud of himself, and he never tried to show that he is more clever than anyone else. For example, he has been receiving many questions on the bitcoin.org forum, related to the Bitcoin design, very much like a beginners question, but he not only replied to everyone, but he always did it with loveliness, and passion. Even if he has been asked the same question, he would let people know where they could find the answers, in case he already replied. Overall, it's fair to say that his written communication was always calm, precise, and considering. Another important quality Satoshi had, which is, he was not financially motivated whatsoever. Satoshi has about 1 million bitcoins on his wallets, and after a decade gone by, he has never touched them, never spent, or exchanged those bitcoins. It all depends of the date of reading this book, but if you consider an average price of the current 16,000 dollars per bitcoin, he has about 16 billion dollars worth of coins which he never touched. Back in 2017, the price of bitcoin was about 20.000 dollars and still he hasn't exchanged or moved not even a small portion of those coins. He could have sold all those bitcoins at any given time, even when it was 1000 dollars, 100 dollars, or even 10 dollars a coin, he could have made a fortune, but he chosen not to. There is also a software pattern, for both Bitcoin and blockchain, which Satoshi could have filed, which itself also worth billions of dollars, but he never did it, in fact he wanted to make sure that Bitcoin and the blockchain is completely decentralized, and open source. I will talk about the Bitcoin code and how Satoshi managed to release it to the public in a later chapter.

Chapter 5 Satoshi's DOB

In this lesson I will cover some of the politics view of Satoshi. There are not much can be found in terms of political view and believes of Satoshi. Yet there is one very important fact that you should know about the Genesis block. In case you not aware what the genesis block is, is basically the first block mined of the Bitcoin blockchain. There are many reasons why the genesis block is important, but the reason I will bring it up, is because the genesis block contains a headline from the January 3rd 2009 edition of ''The Times'' newspaper. The headline is:

''Chancellor on brink of second bailout for banks''

This headline was on the newspaper after the 2008 financial Crisis, when the Chancellor was considering to provide or create more money into the system, which also known as quantitative easing. Quantitative easing is basically the introduction of new money into the money supply by the central bank. Another evidence in relation to political views of Satoshi was announced by himself on the p2pfoundation.ning on 11th of February 2009, which is as follows:

"The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible."

To read the whole forum post, please visit the following link:

http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source

This post by Satoshi tells you that he not happy how the system is running, in terms of money printing by the central banks. There is another piece of evidence can be found about Satoshi's political believes, and that is the on p2pfoundation, where he posted the above announcement. When Satoshi registered to become a user on the p2pfoundation, every new user must provide their date of birth. Satoshi has provided 5th of April 1975. That was back in 2009, so at first sight, most people would think that it could be

Satoshi's actual birthday, which would make him about 34 years old at the time. The truth is that these dates are actually very significant in terms of Money supply and gold. On 5th of April, in 1933, Franklin D. Roosevelt, who at the time was the US President, announced an Executive order by making gold illegal, making every US citizen to deliver all their Gold to the Government. To read the whole article, please visit the following link:

http://www.presidency.ucsb.edu/ws/index.php?pid=14611

Franklin D. Roosevelt the 32nd President of the United States, announced an executive order of Returning Gold Coin, Gold Bullion and Gold certificates to be delivered to the Government. It was around the time of the Great Depression, which started back in 1929 and lasted until the late 1930-s. To read about the Great Depression, you can visit the following link:

https://en.wikipedia.org/wiki/Great_Depression

In terms of the year of 1975, this was a year when the Americans were able to own and trade Gold once again. From 1933 to 1975 it was illegal for a US citizen to own Gold in any form, without a special licence. But these restrictions were lifted in 1975 and Gold once again was freely handed. 5th of April 1975 might be the actual birthday of Satoshi, all though it is very interesting that these dates are correlate with a huge Gold news that taken place in the previous century. It might be coincidence, and Satoshi is just put a random date to the forum, still because he was always so considering, when he was asked to provide his date of birth, probably thought that he not only want to provide some sort of random date, but something that he would remember. Given the fact that Satoshi's main life project was Bitcoin, which often referenced as Digital Gold, and of course a Decentralized blockchain, which government cannot confiscate, take away from people, probably these dates are not a random at all.

Chapter 6 Publishing the Bitcoin Software

In this chapter we are going to cover what considerations Satoshi has taken before published the Bitcoin software. First of all, the Bitcoin software is published under MIT licence, which provides open source software. In terms of open source software, there are different categories. For example one can be published to be a free software forever, and there is another type which provides freedom for the end-user. To be clear, the first example is in a category of a GPU Licence, which referred to as a General Public Licence. You can modify the software if you want to, but it has to be published once you made any modifications with it. While with the MIT Licence, you can make any modifications you want, but you don't have to publish it if you don't want to. Also you can use it as part of any other work or project if you want to, and Satoshi wanted to have the Bitcoin software like that. What Satoshi wanted to achieve with the MIT licence, is basically to get it to as many people as possible, spread it around the globe, and to let it have to anyone and make any modifications as many times as they want to. Making this decision, he was very considering and he must have done a lot of research to know the differences before he would have published the Bitcoin software.

Chapter 7 Satoshi's identity

On the Wikipedia page of Satoshi, he is referenced as an unknown person or people, so I will make a case first that Satoshi was a group of people. One of the main reasons why Satoshi could have been a group of people, which is that in order to create a Bitcoin software, Satoshi had to be an expert or at least very knowledgeable in a wide range of areas, which are: Economics, Distributed computing, Databases, C++ programming, and of course Cryptography. When you think about these skillsets, you can quickly realize that, it is likely to be a skillset of multiple people instead of an individual. For example a Cryptography expert would not necessarily have a skillset on databases, and certainly not on Money theory, or economics, but all thought it is possible. Another example is that an average C++ coder, normally would be studying C++, phyton, or JAVA, but not exactly the history of money, or peer-to-peer systems. I am personally interested of a wide range of topics too, but I am not an expert in all those fields that interests me, so once again, most people just don't have enough time in life to master multiple skillsets. So for that reason it is possible that Satoshi is a group of people. Another example that would indicate that Satoshi is not an individual can be found in the actual Bitcoin whitepaper within the Abstract. Fifth sentence down the line, where he written:

"We propose a solution to the double-spending problem using a peer-to-peer network."

Because it's written in plural, it suggests there are multiple people have been working on the Bitcoin design and implementation. We have already learned Satoshi was always very considering, and maybe he wanted people to think that he was a group of people by misleading anyone who reads the whitepaper. There are some other publications by Satoshi where the sentences are written in plural, but these are the main cases I managed to find.

Chapter 8 Satoshi is an Individual

We already discussed that the Bitcoin design and implementation was a work of a genius, and there is something very common within all genius minds. They prefer to work alone instead of outsourcing tasks or working with a team of people. Another reason why Satoshi could be an individual is because his writing style is indeed very consistent. There are multiple forum posts and e-mail replies, and they just don't appear to be from multiple people. Satoshi's writing style was unique, so if there were other people involved, even just to reply some of the forum posts, they must have follow a certain writing style but it is highly unlikely. Satoshi first appeared online back in 2008, and after a decade gone by still there is no confirmation of Satoshi's identity. If you think about it, imagine when you have a secret, and don't want anyone to know about that secret. If you let some people know about it, you would increase your chances of your secret to be leaked out right? So, the point is this. Satoshi has been considering his name and date of birth while provided no identity information whatsoever, then there is a high chance that he also considered who he should tell about his true identity, and given the fact that he never revealed himself, there is a high chance that he was alone all along. Being realistic by analysing probabilities, there is a much lower chance to stay anonymous if less people aware of you. So when it comes to calculating game theories, probabilities, possibilities, such as calculating increasing difficulty in a hashing power in every 14 days, or creating 21 million bitcoins, by 50 bitcoins in every 10 minutes, but then reduce the supply, halve the supply in every four years, it is highly likely that he never told anyone about the Bitcoin project by his own real identity. As you see I am making a case for both scenarios. Satoshi might be a group of people, but he might be an individual. But considering the level of the Bitcoin Project creation, it is highly possible that he is an individual. If Satoshi is a group of people, I would say that is a very carefully selected, small number of people. Maybe 2-3 people, but no more than 4 people. There is a higher chance that Satoshi is an individual. For example in the Bitcoin whitepaper, he mentions ‘’we propose’’ instead of I propose, on the top of the Title the name is written as Satoshi Nakamoto, and not Satoshi's Team, or other people's name, and there is only one e-mail address provided for contact. At the end of the Whitepaper, there are references for the Bitcoin

implementation, so I think the way he announced his proposal, is that he used all those as part of the implementation of Bitcoin, but he did it all himself.

Chapter 9 Satoshi Candidates No1

In this chapter I will talk about one of the first candidate who thought to be the real Satoshi Nakamoto. In 2014 there was a an article published by Newsweek, with the title: ‘’The Face behind Bitcoin’’ where they have claimed that they found Satoshi Nakamoto, the mysterious missing man, who leaves in California, and his real name is Dorian Satoshi Nakamoto. To read the full article, please visit the following link:

http://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html

Dorian lived very close to Hal Finney, who actually received the first 50 bitcoins from the real Satoshi, but I will talk about this later. There were lots of speculations around that time, that Dorian used to work for the government, and he was some sort of an engineer. He said that he is not allowed to talk about his work with the government, so he became very suspicious for many people and of course the media loved this story and tried to make the best out of it. In the end of the day, Dorian seemed to be not even aware of Bitcoin and he had really no clue about blockchain, cryptography or anything like that. But it was the media who made a big deal out of it. Dorian has denied any involvement about the Bitcoin design or creation, and he was just confused of the whole situation really. There were multiple analysis about his public writings and e-mails, and they realized that Dorian just can not be the real Satoshi, there is just no way. I did say that, I am going to talk about some of the Satoshi candidates, and if you ask me about Dorian; can he be the real Satoshi? I will say no. But the reason I am talking about Dorian, is that because if you don’t do your research properly and read articles like the Newsweek, you could be easily mislead by the wrong information. Unfortunately many people don’t even care who the real Satoshi might be, instead just believe that he is some Japanese guy, and that’s it. Of course there are others who would do a very quick Google search and click on images, to see who pops up, and if you look at an example this search Dorian’s face will come up, but once again he is just not the one.

Chapter 10 Satoshi Candidates No2

In this chapter, I will talk about the second possible Satoshi Candidate, whose name is Dr Craig Steven Wright, or Craig Wright, but most Bitcoin maximalists, just call him fake Satoshi. In order to understand why people call him fake Satoshi, you need to know how Craig became first popular. In 2016, Craig has called the BBC to his home and went front of the cameras to claim that he is Satoshi Nakamoto, the creator of Bitcoin. He also explained that some people probably won't believe him, some might do, but he doesn't care. Moving on, the BBC reporter asked him to identify himself, but the way he did it, it wasn't recorded, and of course the reporter didn't even know what to look for, and so because he never actually exhibited to anyone that he has access to the Genesis block, or at least one of those early Bitcoin wallets that the real Satoshi owned, people began calling him fake, or fake Satoshi. So, before talk any further about Craig, and his current involvement of cryptocurrencies, let's just look at the facts and what we have learned so far about the real Satoshi. First of all, he was always very careful to make sure that his identity remains anonymous, so by inviting the BBC to his home we can all agree that is just wrong. Then moving on by saying that he doesn't care who will believe him it's once again doesn't sound like a real Satoshi. Especially that Satoshi was always a people's person, replied to anyone and explained everything in detail. The same argument applies when it comes to proving ownership. Satoshi invented the Blockchain. He is the master of proof of work, so if he wants to prove something, I mean the real Satoshi, he would do so rightly, so that people wouldn't have any doubt. The real Satoshi would prove who he is to Cryptographers and Cypherpunks instead of a reporter who has no clue what is a public key or private key. The real Satoshi was never after fame. Never acted as someone who would want to waste his time for talking to reporters, or any kind of media. But if that's not enough, Craig became a Bitcoin Cash fan, actively promoting bitcoin cash which is a competitor for Bitcoin. Because of these actions, and started going against the real Bitcoin, people asked him, if he is the real creator, why doesn't he help scaling Bitcoin? But then turns out that he has no clue how to code. In the beginning of 2018, Craig said that he is not Satoshi. In the end, what he said to the BBC reporter is true. Some people believe him, but others might not. The reality is that most people just simply know that he is not the real

Satoshi. Even though he came forward in 2016, it seems that it was only for fame. I could bring up many more examples why Craig is not Satoshi, but I wanted you know that he was very convincing. If you hear him talking, he seem to know a lot in relation to technology, but also realized that he likes to use combined buzzwords that actually make no sense.

Chapter 11 Satoshi Candidates No3

In 2020, there was a lot of new debate about Adam Back who might just be the real Satoshi. Adam Back has a PhD in distributed computing systems which should be the perfect background for building a decentralized computer network. Bitcoin was coded in C++ and Adam codes proficiently in C++. Adam was filing multiple patents a year up until April of 2005 and then he just disappeared until March 2010 which is a full year after Bitcoin was released. Adam was also not writing any academic papers during this time. According to Adam, Satoshi supposedly even sent him the software once it was released. But Adam has never provided proof of these emails. On the Bitcoin whitepaper one of the references are Hashcash which was invented by Adam Back in 1997. The whitepaper for Hashcash was released in 2002 and if you want to take a look at it, please visit http://www.hashcash.org/hashcash.pdf

In terms of Adam's writing style, he uses British English while using double spaces after each period. Adam is also British, born in London and if you remember how Satoshi hidden a political message inside the Genesis block that references The Times newspaper. Well, it is a UK based newspaper. Adam Back is also known for leaving political messages with compact code and he also grew up in London where The Times newspaper was distributed. Adam Back has become a resident of Malta in 2019 and began to show interest in Bitcoin publically since 2013. Adam is a Co-founder of a company called Blockstream and become a CEO since 2018. Blockstream's entire purpose is to hire developers to further the develop the Bitcoin project. The company develops a range of products and services for the storage and transfer of Bitcoin and other digital assets. There was an interview with Adam Back asking him about who he might think the real Satoshi is. He replied:

"Well, I think actually it's better that we don't know because it helps for Bitcoin to be considered like a digital commodity. If there was an identified founder, that thinking would lead lots of people to asking or demanding things. So the fact that the founder is not coming back at this point that takes away that opportunity."

To view the interview, please visit the following page:

https://www.youtube.com/watch?v=688J9UZJxKg

Adam denied to be Satoshi various times and recently said the following on his Twitter account:

“some claim to be Satoshi, days google research blogging stories, and in court, to widespread non-belief.

seems I need the opposite: I am not Satoshi despite recent video / reddit claiming so. some factors & timing may look suspicious in hindsight; coincidence & facts are untidy.”

Adam also said the following:

“it goes deeper - some of what they google researched is true: I moved to Malta, an EU tax haven - in 2009. pure coincidence, though ofc I did know about Bitcoin in 2008 via emails from Satoshi. I was born in London. i do use double-space and native spelling British. can code C++”

“unfortunately silence when usually chatty doesn't help either. can't win! but still not Satoshi.”

To view the entire Twitter discussion please visit the following page:

https://twitter.com/adam3us/status/1259979639092588551

Chapter 12 Satoshi Candidates No4

In this chapter, I will talk about Nick Szabo. Nick is a cryptographer and computer scientist, and he was also part of the early Cypherpunk movement, who also designed electronic cash back in 1998, which he called Bit Gold. In 2013, a researcher named Skye Grey, posted a detailed analysis of text in terms of shadowing Satoshi's writings, and he named Nick Szabo as Satoshi. Skye found that Nick has been using a few terms in his blogs that Satoshi was also using in his whitepaper or e-mails. Such sentences were:

"Timestamp server, or sentences starting like: It should be noted, or expressions such as: trusted third party, cryptographic proofs."

What he said is that, after a quick search for these sentences, he easily pinpointed one person out of a thousand. When they asked Skye how certain that Nick is being Satoshi, he said that he is not certain, but his research on specific terms is pointing his investigations to Nick Szabo. Nick denied to be Satoshi, by he simply said:

"Not Satoshi, but thank you."

At the very first time when began to research on Bitcoin, I came across with the sudoname Satoshi Nakamoto, and I really wanted to find out who Satoshi was, but it's been taken a long time to get some clues from the right sources, and so when I got to Nick Szabo, I truly believed for a long time that he is Satoshi. I have found many clues, and I will not talk about all of them, but a few that I have discovered, which indeed makes a good case. First of all, if you look at Nick Szabo's blog, he is very interested in gold, Japanese history, world economy, cryptography, cryptocurrencies, but what really interesting is that nobody can confirm where Nick lives, where he went to school, where he currently works, or any known previously jobs, no publically known date of birth, and so on. Nick doesn't really go to the media and certainly doesn't talk about himself. Also Nick known as Nick Szabo, but nobody has ever verified that this is his real name, so maybe even the name Nick Szabo is not his real name. Let's look at something else. Considering the fact that Nick was working for over 10 years on Bit Gold, and about the time Bitcoin hit the world, he suddenly forgot about it, it's strange. There is also another clue on the Bitcoin whitepaper on the last page where the references are listed. But first of all, lets see the differences of Bitcoin and Bit Gold.



So, if you take a look at some of the main characteristics, you will quickly realize that not only the name is similar but they are both based upon Proof of work system. Residing on a peer-to-peer network. Participants are earning coins by solving cryptographic puzzles. Every new coins has a timestamp. No trusted third party required like banks or PayPal. Consensus required before moving to the next block, or puzzle. Nick Szabo has designed the Bit Gold back in 1998, but he never implemented it. While Satoshi not only designed but also implemented the Bitcoin network. We know that Satoshi was very supportive, and he never claimed any invention, as he was using existing technologies and put them together in a way that never anyone has before. So, if you take a look at the references at the last page of the Bitcoin whitepaper, you can see that Satoshi referenced b-money, the design of secure time stamping service, Adam Back's hashcash, which is the basics of proof of work, Feller's probability theories, and it's applications, but what is really missing from these references is Nick Szabo's Bit Gold.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

Source: https://bitcoin.org/bitcoin.pdf

So, the question is this: Why Satoshi didn't include Nick's Bit Gold right? If you are completely familiar with a topic, maybe you don't have to include in the references, but Satoshi said later on in one of his e-mails that the Bitcoin is based on Nick Szabo's Bit Gold, so it's a bit confusing. Satoshi maybe wanted that some of us would think of Nick might being Satoshi, so we wouldn't think about other possibilities? Once again, Satoshi carefully planned pretty much everything, so it could go either way. The problem here is that Nick is very much aware of Bitcoin, so how comes that he didn't do anything about it? I mean if you were working on something for 10 years, like Nick was working on the Bit Gold project, and suddenly someone out of the blue just implemented a very similar system like Satoshi did the Bitcoin, and your project wouldn't even be referenced, that wouldn't be weird. But Nick never said anything notable on this matter, so once again very interesting. Another think is that his initials are almost the same, Satoshi Nakamoto, SN, Nick Szabo, NS. To continue this topic, in Japanese the Surname comes first, and it's very common amongst writers, and content publishers that they use sudo names or pen names, and most times they would use a penname that is very similar to their real name.

https://unenumerated.blogspot.com/search?q=japanese&max-results=20&by-date=false

Nick also has been posting a few articles in relation to Japanese markets back in 2005, 2006, and 2007, before the Bitcoin implementation, so we know that he has an interest in Japanese items, and the history of money in Japan, so in theory, Nick could have been thinking to create a pen name in Japanese, a pen name, that's somewhat similar to his real name. So, if you think about the given name: Nick, and looking for a similar name in Japanese, like Nakamoto, and Szabo, maybe Satoshi? It is very much possible, of course it's just a theory. Moving on, everyone who was involved in the Bitcoin project back in the day has released their communication with Satoshi, such as private e-mails, but Nick has avoided doing that, and he also went silent around those months when the Bitcoin software was released. In regards to Nick's Bit Gold project on his forum, he has replied to people who has been reading his posts, and one of his posts when he talked about a potential digital currency, in one of his comments, he asked publically if anyone wants to help him code one up? If you are interested to read the full forum post written by Nick Szabo, please visit the following link:

http://unenumerated.blogspot.com/2008/04/bit-gold-markets.html

So as it seems, Nick wanted to code up his Bitgold project, but there is something that is even more interesting, is that Nick has changed the date of the blog post when he asked if someone could help with the coding from April 2008 to December 2008. So once again, there are multiple accords that pointing to Nick is being Satoshi, yet he denied being the mystery man. Even if you think that these are all strong evidences, maybe just a series of similarities, and incidences.

Chapter 13 Satoshi Candidates No5

In this chapter, I will talk about Hal Finney. First of all, back in 2008, when Satoshi come out of nowhere, he began communicating with people online, but mostly with members of the Cypherpunks such as Nick Szabo, Hal Finney, David Chaum and Adam Back. What you should know is that Hal Finney seems to be the most interested in the Bitcoin project from the beginning, as he was the first guy who was working with Satoshi. They were exchanging e-mails more then anyone else from the Cypherpunk movement. Also, it was Hal Finney who received the first ever bitcoin transaction of 50 bitcoins from Satoshi. So who is Hal Finney right? Hal was a Cypherpunk, a cryptographer, who first got involved in developing the early release of PGP with Phil Zimmermann. Later on, in 2004, he has created his own proof of work system which he called PROW, R.P.O.W., also known as reusable proof of work, while he was working very closely with Nick Szabo and Wei Dai. Unfortunately Hal Finney has died back in August 2014 of the age of 58. He has written a blog post about his involvement of Bitcoin on the bitcointalk forum in 2013, that he's been mining few blocks in 2009 when he was still able to do with a CPU. But eventually he turned off the mining, as he didn't like the Fan noise, and the next time he heard of Bitcoin was late 2010. He said in the same post that he believed Satoshi was a young Japanese American who needed some help, and realized that most of the mid 50's cryptographers were sceptical with the idea. But Hal really liked it, and helped Satoshi to setup the Bitcoin network. He also explained that he has been diagnosed, and have a fatal disease which forced him to retire in early 2011. Hal Finney had 314 posts on the bitcointalk forum, but this was his last post, and if you can find some time, I highly recommend you to read it, as you see there are even today people still replying, or quoting him as a Bitcoin legend.

https://bitcointalk.org/index.php?topic=155054.0

He said the following:

"I thought I'd write about the last four years, an eventful time for Bitcoin and me.

For those who don't know me, I'm Hal Finney. I got my start in crypto working on an early version of PGP, working closely with Phil Zimmermann. When Phil decided to start PGP Corporation, I was one of the first hires. I would work on PGP until my retirement. At the same time, I got involved with the Cypherpunks. I ran the first cryptographically based anonymous remailer, among other activities.

Fast forward to late 2008 and the announcement of Bitcoin. I've noticed that cryptographic graybeards (I was in my mid 50's) tend to get cynical. I was more idealistic; I have always loved crypto, the mystery and the paradox of it.

When Satoshi announced Bitcoin on the cryptography mailing list, he got a skeptical reception at best. Cryptographers have seen too many grand schemes by clueless noobs. They tend to have a knee jerk reaction.

I was more positive. I had long been interested in cryptographic payment schemes. Plus I was lucky enough to meet and extensively correspond with both Wei Dai and Nick Szabo, generally acknowledged to have created ideas that would be realized with Bitcoin. I had made an attempt to create my own proof of work based currency, called RPOW. So I found Bitcoin facinating.

When Satoshi announced the first release of the software, I grabbed it right away. I think I was the first person besides Satoshi to run bitcoin. I mined block 70-something, and I was the recipient of the first bitcoin transaction, when Satoshi sent ten coins to me as a test. I carried on an email conversation with Satoshi over the next few days, mostly me reporting bugs and him fixing them.

Today, Satoshi's true identity has become a mystery. But at the time, I thought I was dealing with a young man of Japanese ancestry who was very smart and sincere. I've had the good fortune to know many brilliant people over the course of my life, so I recognize the signs.

After a few days, bitcoin was running pretty stably, so I left it running. Those were the days when difficulty was 1, and you could find blocks with a CPU, not even a GPU. I mined several blocks over the next days. But I turned it off because it made my computer run hot, and the fan noise bothered me. In retrospect, I wish I had kept it up longer, but on the other hand I was extraordinarily lucky to be there at the beginning. It's one of those glass half full half empty things.

The next I heard of Bitcoin was late 2010, when I was surprised to find that it was not only still going, bitcoins actually had monetary value. I dusted off my old wallet, and was relieved to discover that my bitcoins were still there. As the price climbed up to real money, I transferred the coins into an offline wallet, where hopefully they'll be worth something to my heirs.

Speaking of heirs, I got a surprise in 2009, when I was suddenly diagnosed with a fatal disease. I was in the best shape of my life at the start of that year, I'd lost a lot of weight and taken up distance running. I'd run several half marathons, and I was starting to train for a full marathon. I worked my way up to 20+ mile runs, and I thought I was all set. That's when everything went wrong.

My body began to fail. I slurred my speech, lost strength in my hands, and my legs were slow to recover. In August, 2009, I was given the diagnosis of ALS, also called Lou Gehrig's disease, after the famous baseball player who got it.

ALS is a disease that kills moter neurons, which carry signals from the brain to the muscles. It causes first weakness, then gradually increasing paralysis. It is usually fatal in 2 to 5 years. My symptoms were mild at first and I continued to work, but fatigue and voice problems forced me to retire in early 2011. Since then the disease has continued its inexorable progression.

Today, I am essentially paralyzed. I am fed through a tube, and my breathing is assisted through another tube. I operate the computer using a commercial eyetracker system. It also has a speech synthesizer, so this is my voice now. I spend all day in my power wheelchair. I worked up an interface using an arduino so that I can adjust my wheelchair's position using my eyes.

It has been an adjustment, but my life is not too bad. I can still read, listen to music, and watch TV and movies. I recently discovered that I can even write code. It's very slow, probably 50 times slower than I was before. But I still love programming and it gives me goals. Currently I'm working on something Mike Hearn suggested, using the security features of modern processors, designed to support "Trusted Computing", to harden Bitcoin wallets. It's almost ready to release. I just have to do the documentation.

And of course the price gyrations of bitcoins are entertaining to me. I have skin in the game. But I came by my bitcoins through luck, with little credit to me. I lived through the crash of 2011. So I've seen it before. Easy come, easy go.

That's my story. I'm pretty lucky overall. Even with the ALS, my life is very satisfying. But my life expectancy is limited. Those discussions about inheriting your bitcoins are of more than academic interest. My bitcoins are stored in our safe deposit box, and my son and daughter are tech savvy. I think they're safe enough. I'm comfortable with my legacy.

[edited slightly]"

There is lots of interesting fact around Hal Finney, but there are really three points, or theories I want to share with you. First of all, he was leaving less then 2 miles away from Dorian Satoshi Nakamoto, who I covered earlier that Newsweek claimed to be the real Satoshi. So Dorian was leaving in the same town as Hal, for over 10 years already, which is very interesting. Because of this fact, there is a possibility that Hal used Dorians name: Satoshi Nakamoto, and used him as a patsy, so in case Satoshi would get caught, he would be a ware quickly, as he lived very close to him, so would have known if there is some sort of heat about to come. It is only speculation, but it's very interesting. Another interesting fact is that Hal Finney was forced to retire in the early 2011 due to his illness which he has written about back in 2013. While we also know that Satoshi have left the Bitcoin project around the end of 2010. Once again, very interesting that the dates are somewhat matching, and we can assume that Satoshi might have been choosing to leave the project because he had no other choice due to his illness. Lastly, there is another theory about the First Bitcoin transaction that Hal Finney received from Satoshi. This is my personal opinion, but if I was to build such system like the Bitcoin core, I would test myself without others being involved to ensure that the value is actually transferable. Technically, if I was Satoshi, I would have sent the first transaction to myself using another laptop, just to

see how it works, confirm that is working, and just to see the experience on both end of the transaction: like what happens when I send and what happens when I receive. Because Hal Finney has received the first Bitcoin transaction and he was communicating to Satoshi all the time, maybe, Hal Finney is Satoshi. Hal has also denied being Satoshi, he could have said that he was Satoshi, but maybe he thought is better to keep it this way, not because he doesn't want people to know. But maybe he just wanted to protect his family from potential disturbance from the public, government, journalists, or from anything that could potentially harm them in the future.

Chapter 14 Satoshi Candidates No6

In this chapter, I wanted to talk about another potential scenario, that Satoshi could have been a join venture. A duo of Hal Finney and Nick Szabo. But why would Satoshi being a duo? Well, there are few evidences that are easily can be tied to either of them. But there are comments from both of them that would indicate otherwise. First of all, it is a very well known fact that Hal Finney and Nick Szabo has known each other since 1993, and they been exchanging ideas, and design concepts with each other, ever since. They are both Cypherphunks, both cryptographers, and because there are strong evidences that ties both of being Satoshi, it is possible that they created Satoshi as a result of teamwork. If you remember in one of my early chapters, I mentioned that Nick was asking their blog readers if anyone could help him to code a software, but there was never any reply publically right? What if Hal Finney replied and said, sure I can help you, let's do it together, I will do the coding, and because you already designed the bit gold project, you go ahead with a whitepaper, replying forum post, dev requirements to grown the network and so on. So, maybe Nick said, ok but should we use our name? Hal might have said; let's use a sudo name, perhaps use the name Satoshi Nakamoto just to be on the safe side while working on the project. Its a speculation. But not impossible. Even more interesting is that Hal Finney has created RPOW back in 2004, which is the proof of work for Bitcoin which also not referenced on the Bitcoin whitepaper, same as Nick Szabo's Bit Gold.

To read about RPOW written and published by Hal Finney, please visit the web archives on the following link:

http://web.archive.org/web/20071222072154/http:/rpow.net/

As you see the RPOW is the closest proof of work system to Bitcoin, which is exactly the way that the Bitcoin core in running, and Bit Gold is the closest in terms of game theory and other calculations, technology requirements, like timeserver or solving cryptographic puzzles for coins. Very interestingly neither of these projects are referenced on the Bitcoin whitepaper. Maybe they agreed to leave out their own projects from the references. I might be completely wrong, but as you see the two closest project two Bitcoin is not referenced, while everyone knows that RPOW and Bit Gold is the closest to

Bitcoin, so I just find it very interesting. Lastly, because Satoshi mentions at the beginning of the whitepaper:

“We propose a solution to the double-spending problem, using a peer-to-peer network!”

You notice that he says we! Not I propose, so it indicates that he is not alone.

https://bitcoin.org/bitcoin.pdf

As you see there are many assumptions, still there is a possibility that Satoshi was a joint venture between Finney and Szabo.

Chapter 15 Other Rumours, Assumptions and Theories

In this chapter I will talk about some internet rumours and theories on Satoshi's identity. First of all, I have to mention Gavin Andresen, an American software developer, who is also best known for his involvement with Bitcoin. In 2010 he was declared as a lead developer and only contact for the Bitcoin project. Gavin has been working on the Bitcoin project with Satoshi, and helped to scale the system at the very early stages. At some point Satoshi has e-mailed Gavin and asked him if he could use his e-mail address on the bitcoin.org website, because he was the only contact previously. And Gavin said, sure, no problem, however Satoshi didn't just add Gavin's e-mail address to the bitcoin.org home page, but he also removed his own e-mail address, making Gavin the leader of the Bitcoin project. Not long after, Satoshi sent another e-mail to Gavin, saying that he has moved on to other things and will probably unavailable. Gavin then sent an e-mail to Satoshi that he has been invited to the CIA to talk about the Bitcoin project, and he accepted the invitation, but Satoshi has never responded ever since. Anyhow, Gavin has been designated as a lead developer for the Bitcoin network, but he left the project since February 2016. Gavin has denied to be Satoshi, in fact at some point back in 2016 he said that Satoshi is Craig Wright aka fake Satoshi. However later he regrets his theory due to a lack of evidence that Craig exhibited. Very few people believe that Gavin is Satoshi, but, the majority of the Bitcoin community don't. Other suggestions were made by Ted Nelson in 2013 that Satoshi possibly a Japanese mathematician, named: Shinichi Mochizuki. Ted Nelson have been talking about why he believes in his own theory, but Mochizuki has also denied to be Satoshi. Also heard that Dave Kleinman could have been a possible Satoshi, who was a forensic computer investigator, but he had no connections to the Cypherpunks whatsoever. Therefore there is only a small chance that he could have been Satoshi. Kleinman also has died in 2013. There is another rumour spreading on the internet that Charlie Lee, the founder of Litecoin, is Satoshi, which is actually very interesting. Charlie has created Litecoin back in 2011, and given the facts that Satoshi said he is now moving to other projects around the same time, it is possible that he started working on Litecoin. Also, Charlie has referenced Bitcoin as digital gold, and so he said that now he has created a digital silver, which he named Litecoin. By looking at his background and

expertise, Charlie used to work for Google as a software developer for about a decade, even writing code for the Google chrome browser but in his spare time he created Litecoin, and then moved to Coinbase as Chief Technology Officer. Charlie has left the Litecoin foundation in order to keep the project fully decentralized. Charlie has denied of being Satoshi, but it is possible that Charlie is Satoshi. In 2017 an article been published that SpaceX and Tesla COE Elon Musk, is the Real Satoshi, based on his technical expertise with financial software and history of publishing whitepapers. But in November 2017 Mask denied the claim. Kaspersky lab claimed that Bitcoin is an invention of US intelligent agencies, which was designed to provide quick funding for the US, Brit, and Canadian intelligent activities. On the other hand, there are people come up with all sorts of new theories such as Bitcoin was implemented by the NSA, KGB, Mossad, CIA and Satoshi is a codename for a group of secret service crypto experts. There is very little evidence for this, as these are most likely only conspiracy theories, or propaganda, but there is a very small chance that It’s true.

Chapter 16 How Can Satoshi Prove himself

In this chapter I will talk about how could Satoshi reveal himself, or prove himself on the right way. First of all, one of the main concern is that the greater part of the Bitcoin community who believe is Satoshi, is denying of being Satoshi, and those who came forward of being Satoshi, we just don't believe them. So what can we do about it? There must be some sort of solution right? Well, the answer is very easy. There is a very easy way for Satoshi to prove himself, but of course, this action would have some serious consequences. Satoshi has hundreds of Bitcoin addresses as he owns close to a million bitcoins, so you have to search within multiple blocks to find them. Nevertheless, there is a very famous genesis block, called block zero which contains one of the first Bitcoin addresses that belongs to Satoshi. You can find the block zero by visiting the following link:

https://www.blockchain.com/en/btc/address/1A1zP1eP5QGefi2DMPTfTL5SI

If you take a closer look, you can see that many people have sent bitcoins to this address. So if you look at it, this is the public key, and if you could get the private key-pair to this address, you would basically prove your ownership to this address. Many people speculate, that Satoshi probably lost his private key's and even If one day he would want to come forward, he wouldn't be able to prove himself. That is possible, but if you think about how careful Satoshi was, or how careful they were, I am sure that they are looking after that private key very well, and probably Satoshi will not reveal himself publically. Simply because if he wanted to, he could have done it already. There is also a possibility, that Satoshi has given away his private key, maybe donated to someone, perhaps keeps it very secured and will give it to his son or daughter one day. Even if someone would crack the private key pair for this or any other public key that Satoshi's owns, it would only prove current ownership of that address and not that the person is actually Satoshi.

Chapter 17 How did Satoshi left the project?

In this chapter I will talk about how Satoshi left the Bitcoin project. First, let's look at some of his earlier timeline. Satoshi has began to appear on various forums, in the late 2008, and he was very active in 2009 – 2010, including mining bitcoins, making few transactions, posting, replying publically and sending e-mails to various people. But his last forum post was on the 12th of December 2010.

https://bitcointalk.org/index.php?action=profile;u=3;sa=showPosts

This forum post is the same as his normal average forum posts regards to upgrades of the latest Bitcoin software on what changes he made, so nothing special there. Nothing like, thank you guys for the hard work, I am off for a while, good bye, nothing like that. After this forum post however, Satoshi was still replying e-mails to various people. His last e-mail was sent to Gavin Andresen, which I talked about before, and that was on the 26th of April in 2011. Satoshi wrote the following:

" I wish you wouldn't keep talking about me as a mysterious shadowy figure, the press just turns that into a pirate currency angle.

Maybe instead make it about the open source project and give more credit to your dev contributors; it helps motivate them."

To read the original email, please visit the following link:

https://nakamotostudies.org/emails/satoshis-final-email-to-gavin-andresen/

After this e-mail, Gavin replied to inform Satoshi that he has been invited to speak to the CIA, but Satoshi never replied. Once again, no good bye to Gavin either, he just left. It could be the reason that Gavin mentioned the CIA invitation, but maybe there are other reasons. We don't know exactly. We don't know because Satoshi never posted or e-mailed to anyone explaining the reason why he left. He simply just left and it is what it is and we have to work with what he left behind.

Chapter 18 Why did Satoshi vanish?

In this chapter I will talk about some of the reasons why Satoshi left the Bitcoin project. First of all, there is a possibility that Satoshi left the project simply because he or they have accomplished everything they wanted to. Satoshi always tried to get more and more people involved, and he never praised himself. Instead, he tried to make Bitcoin to be an open source project as much as possible. His intentions were to make Bitcoin decentralized as possible, and within 2 years, he has managed to get enough developers on board, the community become very strong. He never wanted to be the leader of the project anyway, so maybe he figured that now it's time to move to other projects. Another reason maybe why he left is that maybe he prefers inventing thinks, rather than supporting those inventions. It is possible, and it's also common amongst inventors that once they invented something, they rather move on, and try inventing other thinks, instead of supporting existing projects. No disrespect, but maybe Satoshi left because there were better developers then himself and he didn't want to show weakness amongst others. Maybe he wanted to avoid situations, when he wouldn't know the answer for a new problem, while everyone would wait for him for solution. Maybe he thought to himself, what if I will not be able to come up with new ideas for the scalability solution right? I mean the scalability issue was one of the biggest problem back then, of course there are multiple solutions for the scalability issues since, and one of the best I am aware is the Lightning network. But he might have vanished so he wouldn't look clueless, in case the pressure gets high. There is another reason why Satoshi might just left which is a legal reason, a question around a possible prosecution. It is possible of course that the NSA have found Satoshi, and that's why he never said good by to anyone, but maybe there was so much heat, that he realized that he could face long years of jail time and better to get out until is possible. This could be one of the strongest reason as he was always using sudo name, and he never talked about his personal life to anyone that we know of and once Gavin told him about the CIA meeting he never responded. Another scenario is that if it was Hal Finney, or at least he was involved in the development. About the time he got really sick, he could have slowly left the project, while he never told anyone the actual reason for leaving, otherwise those who know him would suspect that he might be Satoshi.

Chapter 19 Does it matter who Satoshi is?

In this lesson I want to discuss why does it matter who Satoshi is. First of all, there is a rumour that Satoshi can stop the Bitcoin project anytime if he wants to. Because he created it, he could basically stop the network anytime. Well, this is not true. There are multiple reasons for this. For example, the current Bitcoin software has been modified so many times that 80% of the code has been changed since Satoshi left the project. What Satoshi has created back in the day, is not the same as today. Therefore, he wouldn't be able to make changes on it. Another reason is that making changes on the Bitcoin software, even if there are upgrades of any kinds, there are multiple implementations has to be taken place in order to make those adjustments. And even if there are adjustments made on the latest version of Bitcoin, it is entirely up to you, if you want to use those updates, or you prefer to run the older code. One thing that I mentioned before, which is Satoshi owns about 1 million bitcoins, and if you make a quick calculation on the total supply of 21 million bitcoins that will be ever mined, you can see that he controls about 5%. So, if Satoshi decides to sell those coins on the open market, you could witness a huge dip in price, and other investors or traders could potentially follow the sell off too. However when there is a price dip, many people see it as an opportunity to buy more, rather than make a big sell. To be fair, we do see huge volatility in the price of Bitcoin, some days we can see 10 even 15% differences by the price going up or down, so we are kind of use to it anyways. So 5% sell off wouldn't be such a big deal. Because Bitcoin is so decentralized, after nearly a decade, a single entity, like Satoshi, wouldn't be able to stop the network even if he wanted to. But if you don't know that, you might speculate that someone can just shut it down. Why does it matter who Satoshi is? It's a good question, but even better question is that, how comes most people don't care who Satoshi is. I mean, most people just buying bitcoins, but never even think about who created it. Some people think Bitcoin is a good investment, or a good store of value, which is true by the way, however people don't seem to care how Bitcoin was born in the first place. I personally heard of Bitcoin multiple times, and the fact is that I wasn't bothered for years, but once I felt I should get on board, I began to research. To be honest it has taken about 3 to 5 months to know enough, before started investing my first 100 dollars in Bitcoin. There are about 10 different kinds of documentary

films on Bitcoin, still most of them fail to mention enough about the inventor. In fact some of them don't spend more then 3-5 minutes on Satoshi. When it comes to Bitcoin or Blochchain related video courses, I have watched over 30 of them and once again, there are no courses dedicated to Satoshi. Most of them hardly mention him. Even those do mention Satoshi, no more than for few minutes. When it comes to Bitcoin books, and probably there are more then 100 books out there, only very few that focuses on Satoshi. I feel that Satoshi deserves to be known and get more respect by people. We should all understand his original intentions, so we can recognize that he was not only a genius because he invented one of the most important technology on the World, (which potentially more important then the internet), but to see that he really changed the world of economy by creating a decentralized currency which has no inflation. Satoshi invented, the first ever cryptocurrency that is truly decentralized, which is running it's own consensus that completely eliminating any trusted third parties by using cryptographic proofs. He solved the double spending problem, as well found solution for the Two Generals Problem, aka Byzantine Generals Problem, by implementing the blockchain technology. Back on track, when you look at the media, they seem to avoid mentioning anything about Satoshi as well. Newspapers or TV channels, all seem to focus on Bitcoin and Cryptocurrencies, and hardly anything on Satoshi. Why is that? Well, the fact is that most people already decided that they will never understand what Bitcoin is. And given that, they won't ask questions about the origin or the background or who might have created it in the first place. People don't care because they made themselves believe they would never understand the technology. Or worse, many people heard once that Bitcoin is a scam so they don't care who created it. People are busy with their life's, and there are very few who takes an extra step, and not only investing or trading, but doing a bit of a research on who Satoshi might be. The reality is that most people except technology as is, and don't try to figure out how it works or who invented it. You might be one of a kind, but most people don't know who invented the first microwave, Television, Radio, Mobile phone or the internet, or technologies such as https, or gmail. Many people just simply don't care in their whole life time. On the other hand, if you made to this chapter, you are one of the kind who wants to know more. If you are a kind of person who want to know more, in the next few chapters I will cover some great resources, such as movies, documentaries, books and websites to learn even more about Satoshi and the Cypherpunk

movement and you will fully understand that they have been trying to create Bitcoin for over 20 years.

Chapter 20 Will we ever meet Satoshi?

In this chapter I will answer to the question that we all have in mind. Will we ever see or meet Satoshi? Well, in one of his e-mails he mentioned he will move onto other thinks, and he never said what things those are, or at least not publically. So what other things can someone like Satoshi move on, who designed and created a technology that's is changing the world. Many companies all over the world talking about Bitocin, blockchain, cryptocurrency so what other things did Satoshi move on to right? Well, there is a theory that Satoshi might have been dead for a while. I hope Satoshi is still alive and one day will reveal himself, and he should get a Nobel price or some sort of award. But unfortunately not everyone is thinking this way. Beside that, even if he wants to reveal himself who would believe him right? For example, if he lost access to his private keys for any reason, he might never be able to reveal himself or prove that he is Satoshi. As a result, there is possibility that we never going to see or meet him, perhaps we might never even going to hear from him again. The fact is that he was always very discreet about his own identity, no pictures provided, no location, no former work or education, and given these facts, Satoshi probably will never reveal himself. Where he is now? Well, because he has very good financial education, and knew lots about cryptography, he might be working on cryptocurrency wallets, or other Bitcoin or blockchain related projects. Maybe he is one of the anonymous Bitcoin contributor using a different sudo name. He could be working on something that is close to Bitcoin, maybe still writing codes, but of course only if he is still alive. CIA, NSA, or any government agency probably has no idea who the real Satoshi is, because if they would find out, they would punish him, and punish him publically, so people would be afraid not to try anything like that again. In any case, I just wanted to give you an idea on what Satoshi might be doing if he is still alive. If you are Satoshi and are reading this, I hope to meet you one day. In contrast, if you are not Satoshi and you try to reach out to me claiming you are, I will assume immediately that you are only claiming to be.

Chapter 21 Additional resources and references

In this chapter I want to recommend some movies, documentaries, books and websites related to Satoshi. First of all, in case you are not very familiar what caused the 2008 financial crisis, I would like to start by recommending a documentary on that which is called: “Inside Job.” If you didn’t watch this documentary film yet, I would highly advise you to do it, so you can have an idea what was happening in the background years before the actual crises came to light. The Inside Job was released in 2010, but if you think that is some old fashioned documentary, I warn you now, this film can be shocking for some, but if you have watched it already, maybe a long time ago, you might give it a go again. Using the following link, you can check out the trailer:

https://www.imdb.com/title/tt1645089/

Moving on the next excellent documentary about Bitcoin and Satoshi I recommend is called: The Bitcoin Phenomenon. Using the following link, you can check out the trailer:

https://www.imdb.com/title/tt4250314/

This is a short, 35 minutes picture released in 2014 focuses on the Bitcoin creation mainly and how Satoshi solved the double-spending problem. It’s a great show to watch and I am sure you will enjoy it very much! Next documentary is called “Bitcoin: The end of Money as we know it”

https://www.imdb.com/title/tt4654844/

This is released in 2015 focusing on the history of money through civilizations, and explains the differences between different types of monies, transferability, stability, security, store of value and so on. The next documentary that you should put on your watch list is called “The rise and rise of Bitcoin” released in 2014.

https://www.imdb.com/title/tt2821314/

This documentary doesn’t focus on Satoshi as much as it should, instead the main focus seems to be the ecosystem of Bitcoin, but it’s a great documentary to check out. There is also another documentary released in 2017 called “Magic Money” with the subtitle “The Bitcoin Revolution”.

https://www.imdb.com/title/tt6467152/

This movie is about 1 hour long and mainly focuses on Bitcoin in our current environment. The ratings on IMDB shouldn't scare you away and the reason I recommend you to watch it is because it's very much relevant to our recent situation in regards to the Bitcoin ecosystem.

I left the best for last, or at least is my favourite documentary about Bitcoin called "Banking on Bitcoin" released in 2016.

https://www.imdb.com/title/tt5033790/

I found this movie to be the best of them all and this is because it focuses on Satoshi more than any other Bitcoin related documentary out there. Even if you have no time to watch them all, I would highly recommend you to watch at least "Banking on Bitcoin". There are few more shows that I could mention, but I found these documentaries to be the best out there.

Books on Satoshi

There are many great books on Bitcoin, cryptocurrencies or wallet technology, but there are only a handful that gives you an overall idea of Satoshi's identity or personality. My first book recommendation is from Phil Champagne called "The Book of Satoshi". This book is a collection of writings of Satoshi, including all his forum posts and personal e-mails that was submitted by those who communicated with him.

https://www.amazon.com/Book-Satoshi-Collected-Writings-Champagne/dp/B00XWXM1O0

You can go ahead searching on the internet and you will find everything this book contains but it could take some time. Instead, why not have it all in one place and get this book. Personally I listened to the audiobook which is over 7 hours long. Moving on, the next book recommendation is called "Bitcoin: The future of money" from Dominic Frisby.

https://www.amazon.com/Bitcoin-future-money-Dominic-Frisby/dp/1783521023

Another great book is written by Nathaniel Popper called "Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money".

Nathaniel is a journalist for the New York Times and once you read this book, you will realize he has done lots of research on the key people of the Bitcoin creators, contributors and provides information that nobody talks

about.

https://www.amazon.com/Digital-Gold-Bitcoin-Millionaires-Reinvent-ebook/dp/B00P6TZLOU

Websites related to Satoshi

First forum you should visit is called the p2pfoundation where you can find Satoshi's page and his old discussions:

http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source

Once you click on his name you will see that his account has been hacked. Satoshi's first post here about Bitcoin back in 2009 has few replies and there is one in 2014 September by someone who gained access to his account, said the following:

"Dear Satoshi. Your dox, passwords and IP addresses are being sold on the darknet. Apparently you didn't configure Tor properly and your IP leaked when you used your email account sometime in 2010.

You are not safe.

You need to get out of where you are as soon as possible before these people harm you. Thank you for inventing Bitcoin."

As you see someone else got access to Satoshi's profile, but this person seem to come across with good intentions by trying to warn Satoshi.

Moving on, the next website that you should visit is called bitcoin.org:

https://bitcoin.org/bitcoin.pdf

This is the website that Satoshi has registered anonymously and this is the very same website where he uploaded the Bitcoin whitepaper.

The next Forum you should be aware is of course the bitcointalk.org forum which was also created by Satoshi.

https://bitcointalk.org/

If you click on the following link, you can see Satoshi's welcome e-mail

https://bitcointalk.org/index.php?topic=5.msg28#msg28

Satoshi had 364 activities on the forum and if you click on his name you can see that he had 575 posts. This site was registered in November 2009 and last

time he was active here was on the 13th of December 2010. There are additional information on this page too such as last posts or last topics started by Satoshi and by clicking on these links you can find all his posts and comments of Satoshi, including the dates and times for each posts. Lastly, if you go to the website called https://satoshi.nakamotoinstitute.org/ you can find all his public posts, private e-mails, previous codes and even famous quotes by Satoshi. If you made it to this chapter, I have special bonus for you, because this website, also has a collection of Literatures from several Cypherpunks such as Satoshi's Bitcoin from 2008, or Wei Dai's b-money from 1998, Adam Back's Hashcash from 2002, Nick Szabo's Bitgold project from 2005 or Smart Contracts from 1995. Then you have David Chaum's publications when he was talking about online cash back in 1989 or blind signatures and untraceable payments in 1982. As you see, you can find plenty of information that was created by the Cypherounks 20 years before the actual Bitcoin was born. On the main page you can also find Hal Finney's posts when he was talking about Digital Cash and Privacy back in 1993 and then in the same year about the double-spending problem. A year later Hal wrote about the design of PGP and by 2004 he also created his own Hashcash based reusable proof of work system which he called RPOW. They are very old publications but these are the roots of the Cypherpounk movements and the Bitcoin creation. Whoever Satoshi Nakamoto is, still alive or not, one person or many, he is one of these authors.

BOOK 4

CRYPTOCURRENCY INVESTING USING HOT & COLD WALLETS

HOW TO BUY, SELL, TRANSFER AND KEEP YOUR CRYPTO SAFE AND SECURED

BORIS WEISER

Chapter 1 What is a Cryptocurrency Wallet

Many people think that a cryptocurrency wallet is where we keep our digital cash, or electronic cash safe and secured, and it's somewhat true, yet there are lot more into that. First and foremost, back in the day when Satoshi Nakamoto came up with the solution for wallet, it was actually called "client", not a wallet. But for everyone's convenience, the nickname was quickly invented which is nowadays only know as a wallet, or cryptocurrency wallet. In the old traditional financial system, when it comes to cash like paper money, we normally keep that in the wallet, or at least we used to, but when it comes to cryptocurrencies, there are no coins in the cryptocurrency wallet whatsoever. This is one of the most common misconceptions, that people believe they have all their cryptocurrencies in their wallet. This is not true of course. What the cryptocurrency wallet does instead is that it provides access to your funds. For example in the case of bitcoins, when you have some bitcoins, you don't have your bitcoins in your wallet, as all the bitcoins are actually sits on the blockchain. However what you can do is that you can access your bitcoins on the blockchain using your cryptocurrency wallet. Once you have accessed your funds, you can do several thinks, which include of checking your balance, withdraw, or exchange to other currencies, even if it's another cryptocurrency or fiat currency. You can also transfer some of your bitcoins to your friend, which is technically speaking would be that you basically assign an access of some of your bitcoins to another client or wallet address. In a nutshell, Wallets are a software technology, which stores your private and public keys and interacts with the Blockchain to allow you to access your bitcoins or other cryptocurrencies. Once you have access to your account, you can send, receive, or directly monitor your balance. I will get into more details on how cryptocurrency wallets work in the next chapter.

Chapter 2 How Cryptocurrency Wallet works

In this chapter, I will explain how a cryptocurrency wallet works. As I mentioned wallets are a software technology, and each cryptocurrency wallets have a private key as well a public key, but what I didn't mention yet, is that each wallet also has is a password. First of all, it doesn't matter what cryptocurrency we talk about, as each coin has its own official release of wallets. For example Bitcoin has a bitcoin wallet, Ethereum has an ethereum wallet, Dash has a dash wallet and so on, but there are also third party wallets, released by other companies, and those could be all sorts of wallets, which could be named something else, other than the actual cryptocurrency they would hold access to. Third party wallet brands are for example: Bred Wallet, Exodius, Jaxx and so on, which I will talk about later. But for now what you need to know is that all wallets are having the same functionality when it comes to the private keys and public keys. In order to better understand what these keys are represent, I will provide an example of an e-mail, and instead of comparing to a general wallet, I will specifically take an example of a bitcoin wallet. For example in the case of an e-mail, you have an e-mail address, which you can send and receive e-mails to and from. This e-mail address would represent your public key of your Bitcoin wallet. Bitcoin public keys, can be provided to anyone, when you wish to receive a payment, and if you send someone a payment, they will see your public key is where they have received the funds. So basically your public key can be online, and you can show it to anyone, similarly to your e-mail address, when it comes to e-mails. When it comes to Bitcoin addresses, they are most times 34 characters long, and consist random digits of uppercase and lowercase letters. Bitcoin public addresses are always start with 1, and never consist an uppercase of O, or a number 0. Neither have an uppercase I or a lowercase of l, this is for preventing mismanagement of the addresses. Back to the e-mail analogy, when you want to logon to your e-mail, you must have a password, but in the case of Bitcoin, you will require a private key and a password in order to access the wallet. Your private keys must be secured and you should never give it to anyone. Your private key is stored in your wallet, which allows you to access your funds. Bitcoin Private Addresses are always starting with a number 5, and they are generated automatically when you install your wallet and receive a public address. So the private key is linked

with the public key, which you can generate your own password. What you must remember is that you must always backup your private key and keep it safe and secured, perhaps not on your laptop and nowhere where others can access it. Best practices are that you write down your private key and make multiple backups and keep it safe and secured somewhere offline if possible. If you have a wallet on your computer and your computer might get hacked or just broken, using your private key, you can regenerate your public key, and have access to your wallet once again on any other computer or mobile device. One thing worth to mention is that your public key is actually an encrypted version of your public key which uses SHA256, which is also used by all banks still today, so basically just so you to know that this is a very secured and wildly used encryption. Bitcoin wallets also have a QR code, which can be scanned with a phone or tablet device. QR codes are make it easier to access your wallets, send or receive founds. Most Bitcoin wallets do support reading a Bitcoin address as a QR code. Bitcoin QR codes are extremely convenient for many purposes. For example in 2014 in Ukraine, when there was a so called "Ukraine revolution" in Kiev, when a series of violent events happened, involving protests, riot police, and unknown shooters; 82 people have died, and hundreds were injured, and many of them seriously. Field surgeries and hospitals were treating the wounded. Blankets and clothing were distributed with vehicles to those who need, but still they needed more support and more money to get help. What happened is this. Ukraine's who lived outside of the country have joint to found the campaign and raised funds to assist those struggle back home. Unfortunately PayPal only allows money to be sent out of Ukraine and international bank transfers could have taken days to complete, they have started a new types of campaign. They have begun to raise funds directly via Bitcoin. Images have begun to appear online on which people were holding up Bitcoin QR code signs to collect donations from anywhere in the world, in any amount, which they were able to receive instantly. They have managed to receive 28000 dollars' worth of bitcoins within 24 hours. If you want to read more about the Ukraine revolution please visit the following link;

https://www.coindesk.com/hold-ukraine-protestors-turn-bitcoin-fundraising/

Chapter 3 The Importance of Cryptocurrency Wallet

In this chapter, I will explain the importance of a cryptocurrency wallet.

There are numerous different kinds of wallets that exist, and certain wallets support different currencies; still, most wallets are only supporting one particular cryptocurrency. For example, imagine that you have an HSBC bank card that you can access your Euros and British pounds; but, you also have another bank card with Bank of America to obtain your US dollars only. When it comes to a cryptocurrency wallet, some wallets can support multiple currencies simultaneously. But why would you need a cryptocurrency wallet? First of all, the whole concept of Bitcoin was decentralization of ownership. For example in a traditional banking system, when you deposit your money to the bank, what happens is that the bank can lend that money to other customers, charging them for a certain fee, commonly known as interest. So, for example you would deposit to your savings account 20,000 dollars today, but tomorrow, you would change your mind or you would need that money in cash; well, the bank wouldn't have it for you right away. This is very bad, but that is how banks work, and you should ask for an appointment, which could take days in order to take your money out in cash. In the other hand, when you have a cryptocurrency wallet, you have access to your funds anytime you want, to all the funds you have and you don't have to wait or rely on any trusted third party in order to make any transfer. Even if it's 100,000 dollars' worth of bitcoins you want to transfer to your friend in the middle of the night on the Saturday, you can do it with cryptocurrencies if you have a wallet. Cryptocurrency wallet will provide you with full control of your funds which is why the saying that "once you have access to some bitcoins with your own wallet, you are the bank". I already explained in my other book called "Bitcoin for beginners" why this is so important and what was the main intention when the Cypherpunks have been working on these concepts for over two decades, which is revolving around the concepts of eliminating trusted third parties. By avoiding trusted third parties, people can create a more robust marketplace which is person to person, business to business, or even person to business style where transactions are fast, secured and fully controlled by only those who participate in a certain exchange of goods or service.

Chapter 4 Online Wallets aka Hot Wallets

In this chapter, I will explain what is an online wallet which is also known as hot wallet. The reason I will start to talk about hot wallets, because this is what I used when I bought my first bitcoins. And there is a possibility that you might do the same if you are a beginner to buy bitcoins. By the way, if you are new to cryptocurrencies, I would highly advise you not to buy any other coin then bitcoins at first. There are just too many scams going around the internet. It's really sad to see how many people losing their money or worse, their lifesavings because they are buying into some so called cryptocurrency which will become better coin than Bitcoin and turns out to be a scam. I will talk about how to avoid scammers and what to look out for when it comes to the crypto market, but for now let's focus on wallet technology, specifically on hot wallets. In terms of hot wallets, you can have one from Blockchain.info which allows you to have access to your bitcoins. As a side note, I do have a Blockchain wallet, in fact, that was my first cryptocurrency wallet. While the Blockchain wallet has limited resources for currencies, I still use it and I recommend it to anyone to start with it. You can have a Blockchain wallet for free on your desktop as well as on your smart phone by reaching the website https://blockchain.info/

Once you arrive on the site, you can click on "wallet" then click on: "create your own wallet". This will take you to the registration page, where you can sign up in no time and buy bitcoins very quickly. You can connect your current bank account and start to purchase your first bitcoins. This is how I bought my first bitcoins and I would highly recommend if you are a beginner. It's easy to use and you can start using your first Bitcoin wallet which is called Blockchain wallet. This wallet does not support all the currencies that you might want to invest in the future, but for now I only want you to focus is on trusted hot wallets and blockchain.info is trusted as it's on the market since 2011. You don't have to purchase anything on blockchain.info but you can generate your first cryptocurrency wallet which supports Bitcoin. The Blockchain wallet also supports Ethereum, Bitcoin Cash, Stellar USD Digital and Tether as of November 2020. I am not recommending buying any of that until you understand what you are investing into, so let's carry on focusing on understand hot wallets first. If you start with a Blockchain wallet, which I highly recommend, do not go

crazy and invest all your savings. In fact I recommend you do not buy any cryptocurrency until you finish this book. Once you do finish this book, create a wallet and have a feel for the technology, how it works, how to buy, sell or transfer preferably starting with a low amount such as 100 dollars or even 10 dollars. I personally recommend you do not invest more than 500 dollars as a first asset; but if you are a complete beginner, you can even start with 10 dollars' worth of bitcoins. In my case I first bought 100 dollars' worth of bitcoins, but if you are new to cryptocurrency and wallet technology you should finish this book first and start investing only once you have a knowledge that require to understand fully how thinks work. Hot wallet is easy to set up but easy does not come with safety. It is also true with a Blockchain.info wallet. For instance, if Blockchain.info gets hacked, the hackers can take control of all the wallets that reside on their platform. It has occurred before with other trading companies which resulted in bankruptcy. Therefore, you have to understand that any online platform exists today is never 100% secured. Also, once you have a wallet installed on your mobile phone or desktop computer, those devices also can also be hacked. I am not saying that once you buy bitcoins you will be hacked right away but there is a potential risk and you have to be aware of that. If you back up your hot wallet, you have a better chance of being able to retrieve your funds in case something bad happens. But when it comes to hot wallets, it's generated to you by a trusted third party which in this case blockchain.info and they could basically access your wallet. Of course we all trust companies like blockchain.info, or any other online trading platforms, however if they get hacked the hackers can access all the wallets, and they can empty them. Bitcoin exchange hacks already happened with many companies and I will cover those later on but you have to understand that online wallets are not fully secured. In fact if you don't have your own hardware wallet, you shouldn't say that you have bitcoins or other cryptocurrencies. Basically you own bitcoins when you own your private keys. For example if you lose your private keys to your blockchain.info wallet, and tell them by logging a support ticket and explain that somehow you have managed to lose your private keys, basically they can recover it for you. Which you might think it's good and helpful, but in reality the point of having cryptocurrencies is that you are the only person who has the private keys, not a company where tens or hundreds of people working. Also, let's imagine that blockchain.info, or any other online company where you keep your cryptocurrencies are

suddenly inaccessible. For example their website has too much traffic because the prices are down many people wants to buy in the dip, what will happen is that the website will not be able to let you on the platform, which I has happened with me many times on Kraken, on Coinbase, and on blockchain.info too. Websites like these can also just close down and file a bankruptcy if they want to or if they have no other choice, which has happened before with many companies. So, either way, my point on hot wallets is that they are very convenient and very easy to setup and of course they are secured. But I should say that they have a limited security which can be breached, therefore I do not recommend keeping large funds on hot wallets or even small amounts for long term.

Chapter 5 Paper Wallets

In this chapter, I will explain what is a paper wallet and some of its pros and cons. First of all, Paper wallets are also easy to use and provide a very high level of security while they are used offline. Basically you can create your own wallet online that contains your private and public keys, and then print it out. It's basically a free wallet, so one of the pros that you don't have to pay for it, or register anywhere really in order to have one. You can literally have a piece of paper that you can carry with yourself anywhere which holds your funds. Downside to paper wallets is that if you lose them and didn't memorize your private keys, you will lose access to your bitcoins. This is why is recommended to have multiple backups of your private and public keys. Another issue is that once you have generated a paper wallet online, it is recommended not to use it online again. If you want to create your own paper wallet online that's fine, though it is insecure to be used online again, as hackers can get to it. Because the private keys have been generated online, it's very difficult to trust and find a site that is fully secured. If the website was hijacked while you have generated the private keys, you can face a potential danger by the hacker could modify or create a specific key, instead of you are generating a true legit randomly created key. Your computer could be infected with spyware or some sort of malware which could monitor or log all your activities, sites you visit, passwords, or private keys that you typing or saving on your computer. Any of these information could potentially be stolen by someone remotely controlling your computer. If possible, web based generator should not be used to create a paper wallet and it should be kept hidden away from even your web camera, so that no one would ever steal your funds. Because of all paper wallets are rely on centralized lookups when redeeming the funds, paper wallets are not recommended, because people can ruin their own privacy. This is also the reason I do not recommend to have a paper wallet especially that contains large amounts. You might choose to create your own paper wallet for fun, but I do not recommend any website, also highly advise you to do your own research before participating in such activity.

Chapter 6 Desktop Wallets

In this chapter, I will explain what a desktop wallet is. Desktop wallets are practically secured; but they can only be used on your desktop computer. Once you have installed it on a particular computer or laptop that will be your only device where you can access your Bitcoin address. It's not cloud based, and if you regularly turn off your pc and having an antivirus, you should be just fine. Still, there are several ways for hackers to get hold of your desktop wallet using various phishing attacks or viruses from drive by download sites or torrent websites. Once the hackers have access to your private keys, they would be able to access your digital currencies; therefore, it is not recommended for long term use or even for short term when it comes to large sums. Desktop wallets are easy to download and to be used; yet still not fully secured. Desktop wallets, used to be fun, nevertheless most people I know, they don't use desktop wallets anymore, and the reason is pretty simple – they are not fully secured, and this is why I do not recommend any desktop wallet.

Chapter 7 Mobile Wallets

In this chapter, I will talk about mobile wallets. First and foremost, there are many different kinds of mobile wallets and Blockchain.info has one as well. Blockchain.info provides both; online and mobile wallets too. On the other hand there are many mobile wallets exists, which are specifically invented for cell phones only. Having a mobile wallet is essential for making payments anywhere you go, as your cell phone probably will be on you most of the time. Mobile wallets are great to check your account anytime pretty much anywhere where you have internet access. Mobile wallets can provide decent security too; but you must back up your mobile wallet, same as your desktop wallet. For example, if you were to lose your phone or break it, buying another phone and having backup phrases to your private keys, you can simply back up your new cell phone like nothing happened. Nevertheless, if you don't back up your mobile wallet, you can lose access to all your bitcoins forever. Mobile wallets are also in a category of hot wallets; therefore they are not fully secured. Hackers can use many techniques to remote access your mobile wallet, therefore it's not recommended to have large amounts on it or even small amounts for long term. Especially, android cryptocurrency wallet users are at risk from hackers because there is a new vulnerability, which allows to capture the users screen and audio content. This is a bug which effects Lollipop, Marschmallow, and Nougat platforms. There are countless of incidents where people's mobile wallet was emptied without even the owner's knowledge. I do recommend to have a mobile wallet, but I do not recommend to keep more than few hundred bucks on it, as you can get hacked anytime, and in a matter of seconds all your founds can be stolen. I personally use 2 mobile wallets. One from blockchain.info and the other from coinbase, but I try not to keep any cryptocurrency on them, especially for longer than a day.

Chapter 8 Cold Wallets

In this chapter, I am going to talk about cold wallets. Cold wallets are also known as hardware wallets. Both descriptions are often in use and they really mean the same thing. I will cut to the chaise and tell you right at the beginning that you must have a hardware wallet if you are planning on purchasing large sums of bitcoins or other cryptocurrencies. They are the best and safest wallets that you can have. Hackers can't do much by attacking it from online as the cold wallets keep the private keys on the hardware, away from the internet. Some of these wallets often look like a USB stick, and unfortunately, people believe that having a USB stick is same as having a cold or hardware wallet, but this is not true. A USB stick cannot be backed up; neither understands the current market valuation of the currencies. A USB stick is good to keep your private keys on it, but it will not run a wallet for you. For example a USB stick will not let you send or receive bitcoins or any other cryptocurrencies; simply you will not be able to make any transactions with it. Hardware wallets do look like USB devices, but once again, even that is a common misconception that they are the same, they are not. Hardware wallets also have to be connected to the internet for sending funds; but they can be offline when receiving funds. In order to connect a hardware wallet to the internet, it requires a special type of USB cable. Any cryptocurrencies that you are frightened to keep on a hot wallet like mobile or online wallet, you should keep on a cold wallet. There is no way for someone to hack your cold wallet unless they have physical access to it. Even if hackers would have physical access to it, still they must figure out your pin code, and only then would have access to your secret keys. Secret keys are normally 24 random words generated by the hardware wallet that you write down on a piece of paper when you use the device the first time. The only downside to the hardware wallet in my opinion is that if you want to sell some of your bitcoins quickly, you cannot. If you have your cold wallet with you and there is a desktop pc around, then it can be done in less than 2 minutes, still when you have a mobile wallet, transactions can take less than 10-15 seconds. Traders always have lots of bitcoins on their mobile wallets in case they feel like it's time to sell or buy. I call myself an investor when it comes to Bitcoin or any other cryptocurrencies, and I do believe that Bitcoin will continuously increase in value, and while it does, Fiat currencies will

steadily decrease in value; therefore, it will provide an additional boost to the value of Bitcoin to grow even stronger. Hardware wallets are the most secured wallets, there is no doubt about that; but at first, it can be difficult to understand how cold wallets work. Once you have a cold wallet, you have to create your own four digit Pin code, which of course you should remember. Next, the device will ask you if you are backing up an existing wallet or creating a new wallet. When choosing to build a new wallet, the device will generate 24 random words that you must write down on a piece of paper. Normally when you buy a hardware wallet, a piece of paper comes in the box, which also known as a seed or seed recovery sheet. Once you have written down the 24 randomly generated words, which I might add are your private keys, the device will ask you randomly some of those words in order to confirm that you are proceeding correctly. I would advise you that while you generating your private keys, those 24 random worlds using the hardware; you should make sure that you are not typing them to your computer, instead writing down on a recovery sheet or somewhere offline. Also while you are generating your private keys, the device should not be visible to your webcam, or anyone, or even better is to cover your webcam in case you have a malware or spyware on your computer. Sorry if you feel that I am over-exaggerating this part, but it's very important that you do not share the private keys with anyone, and especially online. Do not e-mail those words to anyone and do not upload it to the cloud. Or if you do upload it somewhere, make sure that those 24 words are not together in the same location. Once you have generated the private keys, and confirmed with the device, you have to update the firmware. This is basically a simple hardware update and it won't take more than five to ten minutes, but the point is that you should run the latest update, making sure that you have no unpatched vulnerabilities on your hardware wallet, and running the latest code. After the firmware upgrade, you have to choose what type of cryptocurrency wallets you want to download on your hardware. Wallets such as Trezor or Ledger Nano S can support five different cryptocurrency wallets at the same time. You can choose from more than five cryptocurrencies; but each hardware wallet only will support 5 cryptocurrency wallets at the same time. Technically they support between 3-6 coins but it depends of the size of the application. Let me give you an example. Let's say that you want to have Bitcoin, Litecoin, Monero, Dash and Zcash wallets on your hardware which is not a problem. But a week later you want to add an additional wallet to

your hardware, for example an Ethereum wallet. Basically you will not be able to do so until you delete one of the existing cryptocurrency wallets. If you don't delete one of the existing wallet from the hardware and trying to download a new Ethereum wallet in this case, it will continuously trying but it will fail to install the app. Therefore make sure you have enough space before you would initiate a new download. There are pros and cons to it; but to setup a cold wallet it might require you to allocate 30-40 minutes for these purposes, in order to make sure you do everything right. Installing a mobile wallet is less than a minute but you have to respect the security that comes with a hardware wallet. Furthermore, if you lose your hardware wallet or break it, you might choose to purchase another one, and having those 24 random words you have previously written down, you can re-install all your cryptocurrency wallets in no time. A cold wallet is an absolute must have, especially if you are thinking to become a long-term investor in Bitcoin or other cryptocurrencies. Even though I keep on telling you that you must have a cold wallet, there are a few other cons that you should be aware of, or you should prepare for. First of all do not keep the recovery sheet in the same place where you keep the hardware wallet. Imagine you have a burglary at your home and the criminals find your hardware wallet, while next to the device is another piece of paper that says: "Recovery Sheet" which contains those 24 words you wrote down. They don't even have to take your hardware wallet. All they need is the recovery seed. As I mentioned earlier you can recover your wallet using another device that is compatible with the one you have. Simply typing those 24 words you will have access once again. So you can lose your hardware wallet. It's not a big deal. But you definitely don't want to lose the recovery sheet; especially you don't want it to end up in the wrong hands. As you see, even if it's the most secure wallet ever; still, all can be lost by not taking extra measures. Let's look at another example. This time there is a fire in the building where your hardware wallet is. Again, it is good to have a recovery sheet; but if that gets lost for any reason, well, if you still have the device, you have two choices. One is to look after that device forever, or another is to send every fund to another device that is backed up. So you should make sure that you have multiple copies of your recovery sheets, and try not to scan it in, and try not using printers that are connected to the internet. You might choose to put the recovery sheet in the cloud, so you can access it in the future at any time; but having all those 24 words together is not such a good idea, especially keeping them online. What you

can do is this: Keep six words on Evernote, another six words on Facebook, another six on Gmail, and another six on Yahoo storage. This is just an example and of course you can come up with your own way of doing this, it's completely up to you. Let me tell you another issue with too much security. Let's assume that you are a male and you have a wife who isn't really into the cryptocurrency world like you or me. Most likely your wife has no clue what Bitcoin is, not to mention hardware wallets or recovery seeds and platform exchanges. Let's imagine that you have 2 bitcoins and each coin worth around 10000 dollars, but something happens to you. Let's say that you end up in the hospital. I apologies to come up with the worse examples but my point is this. There is no sense to save all that cryptocurrency for your son or wife if they never going to be able to access it. So, because you put the recovery sheet in 4 different safes, and each safe is in different banks and each bank is resides in various countries, you might choose to have so much security that not only hackers, but even your loved ones won't be able to access those funds ever. What I am trying to explain is that you should teach your loved ones or you should tell them that you have written down a step-by-step guide on how to access those funds in case of an emergency. Either if you end up in the hospital or if they would lose the hardware wallet, you should have a plan for emergency. Even if this emergency situation is never going to happen it's better to prepare for it then not to have a plan at all. I understand that probably not everyone will make a plan; it's not a best thing to spend time with preparing for the worse. Nevertheless, I think it's worth mentioning to you so you can decide how to go about it. Sales pages on blogs like compare websites or YouTube affiliate sales people will never going to tell you these as a con because most people only want you to buy these wallets using their affiliate links. Still I truly believe this is something worth thinking about. My final word is that hardware wallet is the way to go about cryptocurrencies, but it's good to be aware of all the cons as well instead of talking only about the pros. In the later chapter I will explain the differences between the various types of hardware wallets, how to purchase them and what to expect in terms of prices and delivery times.

Chapter 9 Tips to choose the right Wallet

In this chapter, I will talk about some of the major indicators that will determine what kind of wallets you will require. Now that you are aware of all different types and kinds of wallets that exist on the market, it's time to get one. First and foremost there are few questions that you should ask yourself before choosing a wallet:

1st question: Do you need a wallet for multiple cryptocurrencies or only for bitcoins?

If you are a complete beginner and want to get into the Word of cryptocurrencies but don't know where to start, I would advise you to start buying bitcoins first. If you have a limited knowledge on Bitcoin, you can always check out my other book called "Bitcoin for Beginners", or "Bitcoin is Blockchain and here is why!" The reason I am mentioning is that if you are not fully understand what you are investing into, it's better to do more research instead of losing your money. Unfortunately, many people start buying "tron", "monacoin", "verge" or other scam coins because they are cheap and believe they can become a millionaire in no time. Then losing their money because turns out that these coins were a scam. Bitcoin exist for over a decade already, so would advise you to start buying bitcoins at first and then maybe monero or litecoin, but you really have to do your own research. Either way, most wallets support Bitcoin, so you will need a hot wallet and a cold wallet too.

2nd question: Do you want a wallet to hold your crypto for long term? For example you want to keep on buying cryptocurrencies and hold onto them for a long a time?

If this is the reason you need a wallet, then my answer is that diversification is good, but instead of having 10 different kind of cryptocurrencies, and later realizing that half of them has no use case in the future, then you have get rid of them, which is pointless. But if you are planning to keep on holding cryptocurrencies for long time, hardware wallet is the way to go about it.

3rd question: Are you planning to get paid in bitcoins?
The reality is that many people already planning to get paid in bitcoins in exchange for their services, or goods that might be selling online, or even offline.

If you are planning to have a business where you planning to get paid in bitcoins daily, you will need multiple hot wallets, so you can see the transactions immediately. Probably good to have multiple mobile wallets, and if it's an offline store, where you are planning to accept bitcoins, like a restaurant, or an off-licence shop, you should have multiple mobile wallets on phones and tablet devices too. If you perhaps planning to pay wages in bitcoins, it's the same case; you will need multiple hot wallets but at least one mobile wallet.

4th question: Do you wish to have anytime access to your cryptocurrencies?

I will not get into examples, but the answer is that you will need hot wallets, most probably mobile wallets, perhaps having multiple phones, and multiple wallets on each device.

5th question: Are you planning to trade multiple cryptocurrencies in a daily basis?

If that's the direction that you are going to, then you will need many things. It depends on what kind of trader you want to become, like a day trader in fulltime, or you just planning to spend few hours trading on the weekends. Nevertheless when it comes to trading, you most probably will have to have multiple hot wallets on multiple platforms, as well multiple mobile wallets on multiple devices. In case you are thinking why mentioning multiple wallets and multiple devices, there are different reason for different situations, and I personally have learned the hard way. For example, when Bitcoin last time went down from 9K to 4K, I wanted to buy quickly, but platform called Kraken was unreachable and the situation was the same with Blockchian.info and Coinbase too. There were too many people who tried to access these websites, which basically caused the website to be unreachable. It's very

similar to a DOS or Denial of Service attack. At the time I was on holidays and I felt that if I don't buy right now, by the time I can get back to a computer the price will probably go back up. I was on my way to the airport from a hotel which took me an hour, then quickly had to check in. The flight has taken 3 hours and by the time I was able to buy bitcoins, the price has gone back up to 6K. Because some of the most known platforms were down, especially the ones I was registered on, I couldn't buy bitcoins for the price I wanted to. Since, I have registered on other platforms too such as Binance, Bitfinex and Cryptomate too, so I have a better chance for the next time when I want to buy the dip. What you need to know is that each of these platforms the registering is free, however all these platform are performing their own kind of KYC, stands for "Know Your Customer". Basically they would ask you to provide a proof of Identity and some sort of proof of Address, which is a law for money laundering purposes. Even that I have all those details, the verification process can take some time, and the fastest I have ever experienced was 4 working days with Blockchain.info. So, that's one situation when you are planning to buy and unable to do so. But if you have a business, like a restaurant and the customer is about to pay with bitcoins, you must have multiple hot wallets so even if some of them wouldn't work, you should be able to have at least one that works in case there is a network congestion. Also if you are planning to accept cryptocurrency payments, you should have multiple wallets that support other cryptocurrencies then just bitcoins. For example litecoin become very convenient as a payment method, due very low fees. In the other hand there are people who don't want to be involved too much. Instead only want to invest and hold bitcoins for a long term. This is the easiest approach to cryptos and you don't have to do much. For example you can simply just purchase 100 dollars' worth of bitcoins in every month and sit on it. Even if it goes down in price or goes back up, just buy 100 dollars' worth in every month and in the long term you will have some saved money which could be very helpful for your retirement. If this is what you are also planning, you will need at least one hardware wallet, and probably at least one mobile wallet. I know most people just want to have a wallet and see what happens, but you should go through your plans, even if they are short term or long term and plan a head. Once you have settled and

understood your need and future requirements, you can choose the wallet or wallets what best fit you. In the next section I will cover my recommendation when it comes to wallet technology and the best choices that you should consider.

Chapter 10 Blockchain Wallet Online Installation

In this chapter, I will talk about the blockchain wallet. I have explained already how the Blockchain wallet works and its limitations when it comes to cryptocurrencies. The Blockchain wallet is only able to hold a few cryptocurrencies but this is my number one recommendation to anyone in terms of hot wallets, especially if is going to be your first cryptocurrency wallet. The reason I am recommending the Blockchain wallet is because it's one of the most well-known and reached platform around the world. It all depends in which country you are at, but Blockchain.info is the most popular wallet in the world and its accessible from anywhere around the world. The platform can be reached on https://blockchain.info/

Once you enter the site, click on "Wallet", and then sign up. Next you have to provide few of your details but the procedure is very straight forward. First you have to provide your e-mail address and create a password then click on continue. When you are on the platform, you should navigate first to settings, then security, and enable two-step verification. Next you should go to "Wallet", then click on "recovery phrase", and click on "BACKUP PHRASE". This is for just in case you will need to recover your wallet for any reason. After that, you can click on the next step which will provide you 12 different wallet phrases. Once you create your own wallet, you really should write these 12 words down and preferably do not keep them on your computer. Instead, write them down on a piece of paper and keep them somewhere safe. Next, you can navigate to "general settings" where you can pair your online wallet with a mobile wallet. Here, in the general settings you will see: "Mobile app Pairing code". Click on that. Next you will have an option called "show pairing code". If you click on that, it will show you a 3D QR Code that you have to scan with your mobile device once you downloaded the blockchain.info application from the IOS APP Store or the Android app store. While you at the online wallet, you can click on the dash board where you can see your balances and the price chart and below you can see your recent activity. Next, below the dashboard, you can click on "Bitcoin, Ether or Bitcoin cash, which displays all your transaction history. Or you can navigate down below to the menu called: "Buy & Sell Bitcoin" where you can quickly place an order through the platform, by entering the amount, then clicks on buy Bitcoin, and click on "Continue". As you see it's

very easy to buy bitcoins or other cryptocurrencies. Or, if you want to sell your bitcoins to exchange them to Fiat currency, this is where you can do that. You can also click on the menu called: “Exchange” where you can exchange between cryptocurrencies. For example you might have bought some Ether that you want to exchange to bitcoins or vice versa, the “Exchange” menu will allow to do that.

Chapter 11 Blockchain Wallet Mobile Installation

In this chapter, I will explain how to install the blockchain.info wallet to your mobile device. Once you have created an online wallet on Blockchain.info, next you can have the app downloaded from Google Play Store and pair your mobile device with your online wallet. First, go to your Google Play Store and search for Blockchain to find the app. Make sure you get the correct one not some fake wallet. Next click on the option called “install”, and then just wait for the installation to finish, and then click on “open”. At first you can create a wallet, where you can type all your details, but if you already registered your online wallet, you can just click on log in. This will take you to the next page where the app will ask you to pair the device with your online wallet. In the previous chapter I explained that under General settings, you can click on the menu called: “show pairing code” which will bring up your 3D QR code that you have to scan with your phone or tablet device. Once you have scanned the code, it will synchronize the wallets. Once that’s complete, the app will ask you to create a 4 digit pin number which you have to retype once again, and then the app will decrypt your wallet. After the pairing you will synchronize your mobile wallet with your online wallet. Next, you can click on “transactions” where you can see all your previous transactions. You can click on “Ether” where you can see all the Ether transactions, but you can click on any of the transaction that you have made previously and you will see the value when it was sent or received in dollars or any other Fiat currencies you choose. You can also put descriptions for each transaction. For example write a note why a specific amount was sent or received. You can also see the exact date when the transaction was confirmed and you can verify it on the blockchain if you click on “verify on blockchain.info”. This will take you to the next page and show you all transaction details, such as the addresses was sent to and received from, the size of the transaction, inputs and outputs and some more other technical details like the script. Also, if you go back to the “wallet” menu you can click on the “dashboard” where you can send bitcoins by entering the amount in either dollars or in bitcoins, and then enter the Bitcoin address. Or, if you have the 3D QR code of the recipient, on the top right corner you have an option to scan it in. If you go back to the dashboard, you can check the value of bitcoin for the last day, last week, last month or even for the whole year.

On the top left corner there is another menu option called ”Additional Features” which once you click on you will have most of the features that you have on your online wallet as well. Within these advanced features you can select “your local currency”, “2 step verification” and “screenshot enabling” as it’s disabled by default. Then you can click on the menu called “Exchange” where you can exchange between your cryptocurrencies. You can also double-check your backups but if you see “my backup is complete” then don’t have to worry. “Bitcoin addresses” menu option allows you to import additional Bitcoin addresses if you have some more and here you also have the option to scan the 3D QR codes. You can also request a unique amount of payment if you want to but that’s pretty much it when it comes to a mobile wallet that blockchain.info provides.

Chapter 12 Coinbase Wallet Online Installation

In this chapter, I am going to talk about the Coinbase wallet. First of all, Coinbase is one of the most known online exchanges on the world. It was founded in 2011, same as Blockchain.info and anyone can have a Coinbase wallet anywhere on the world. Coinbase has an online wallet and a mobile wallet similarly to Blockchain.info and it's also very user friendly. Coinbase wallet supports Bitcoin, Ethereum, Litecoin and Bitcoin Cash. Once you navigate to the website called https://wallet.coinbase.com/ you can click on "Wallet" and sign up. You have to provide your name and e-mail address and a password, and then click on create an account. Coinbase has investors such as New York Stock Exchange, BBVA, USAA and many other banks too, so they have also opened another platform called GDAX. GDAX stands for Global Digital Asset Exchange which is more like a professional trading platform while Coinbase is for average customers who can buy, sell or store digital assets. Once you register on Coinbase, your credentials will also work on GDAX as well. After you have created an account on Coinbase, you should go to "settings" and then click on "security". Here, you have to provide your phone number and enable two-factor authentication for better security. Next, you can go to the Dashboard and see the current price of Bitcoin, Bitcoin Cash, Ethereum and Litecoin. Under the option called "buy/sell" you can also buy and sell any of these cryptocurrencies. Under the menu option called "Accounts" you can view your accounts of each cryptocurrencies. Under the "tools" option, you can create multiple Bitcoin or Ethereum addresses. You can also create recurring transactions, you have also a reports and the history of transactions but that's really it. In the next chapter, I will explain how to download the Coinbase mobile wallet to your smart phone or tablet device.

Chapter 13 Coinbase Mobile wallet Installation

In this chapter I will explain how you can install the Coinbase mobile wallet. Once you have your mobile phone ready, navigate to Google Play Store, search for Coinbase wallet and click on install. Wait for the installation to complete, and then click on “open”. Next, click on “Sign up” but if you already registered for your online wallet you can just click on “log in” and enter your e-mail address and password that you used when signed up at the first time then login. The next page will ask you for two step Verification code which you will receive in SMS text format. Then you have to enter the verification number, and click on “verify”. Once that’s complete, you will see your fully configured account. You can click on any of the cryptocurrencies and see the current price or you can buy and sell. Very similar to Blockchain.info wallet.

Chapter 14 JAXX Liberty desktop Wallet Installation

In this chapter, I will talk about the JAXX Liberty wallet, formerly known as Jaxx wallet. Jaxx is one of the most popular mobile wallets and to be honest, everyone's favourite. Jaxx supports multiple currencies such as Bitcoin, Ethereum, Ethereum Classic, Litecoin, DASH, Zcash and Monero. Jaxx supports 8 different platforms, including Windows, Apple, Linux desktop, Android, IOS mobile and tablet, Google Chrome and Firefox extensions as well. Jaxx has an excellent user interface which is comfortable and easy to understand, therefore it has very user friendly experience. If you have it on multiple devices, Jaxx will synchronize to them all, similarly as the Blockchain wallet does. On the downside, Jaxx appears to be slow sometimes and this is because it is not open source software and it also supports multiple currencies. Jaxx can be found at: https://jaxx.io/

When you visit the site, you can choose from the supported platforms and once you are ready you can click on download and choose the wallet according to your existing device. For example if you have a Windows machine, click on "download" and it will start to download your desktop wallet which can take a few minutes, it depends on your internet connection. Once the download complete, you can click on the menu option called "install" and click "continue". Next, you can choose to create a new wallet or pair an existing wallet. Next you can choose the express setup, and then choose what wallets you wish to have. There are plenty of wallet supports with JAXX, not like Blockchain.info or Coinbase, as you can setup wallets for cryptocurrencies that you perhaps never even heard of. For example you can choose to have a Bitcoin wallet, Ethereum wallet, a Litecoin wallet, a Dash wallet and a Zcash wallet. Next, click on "take me to my wallets" option and that's it. You are done. You can now send or receive bitcoin. You also have your 3D QR code, same with other wallets too. In case you want to add more wallets, on the right side you have an option by clicking on "Wallets", and then choose whatever coin you want to have wallet for. It's super easy. You don't need an e-mail address and you don't need to register for JAXX. JAXX supports way too many cryptocurrencies. Each of these cryptocurrencies has different platforms and JAXX supports and compatible with them all which is great. One thing you might be missing though? That's right; there is no option for buying with Jaxx. All you can do is send or

receive cryptocurrencies. What you have to do really is send some bitcoins to this address, and exchange them to any other cryptocurrency you want to have that JAXX supports. I do recommend JAXX to anyone as it’s a great wallet that supports many cryptocurrencies on the most popular platforms so hopefully you will download and setup your own JAXX desktop wallet.

Chapter 15 JAXX mobile Wallet Installation

In this chapter, I will explain how you can download and install the JAXX mobile wallet. Same thing as before with other wallet examples, go to Google Play Store and search for JAXX blockchain wallet. Next, click on “install”. Wait for the installation to complete and click on “open”. It might take some time to open the app but once complete just click on “continue”. Next, you can pair the devices like we did with both Coinbase and Blockchain.info wallets. But if you only want to have JAXX on your mobile device like most people do, just click on “create new wallet” and continue. Next, choose the cryptocurrencies that you want to have a wallet for such as bitcoin, ethereum, litecoin or dash, and click on option down below called “take me to my wallet”. Next, Jaxx will create the interface for those wallets you have chosen, and that’s it. You have all the wallets you have chosen. But, it’s the same thing as on with the desktop version, you can add more wallets if you want to.

Chapter 16 Exodus Wallet

In this chapter, I will talk about the Exodus wallets. I already demonstrated how to download and use some of the most popular hot wallets; however there are many more that you can choose from. So, instead of demonstrating how to download and install on your desktop, I will try to keep it short and just cover some of the basic information that you have to be aware. If you like the exodus wallet, you can download it from their official website by visiting https://www.exodus.io/ . Exodus wallet is another hot wallet that you can download for free and start using it right away. Exodus supports, Aragon, Augur, BAT, Bitcoin, Bitcoin Cash, Civic, Dash, Decred, District0x, EOS, Ethereum, ETH Classic, FunFair, Gnosis, Golem, Litecoin, OmiseGo, SALT and many more. As of November 2020, Exodus supports 124 cryptocurrencies. Exodus is available to download on platforms such as Windows, Mac and Linux. Same as JAXX, Exodus is also a multi-currency wallet, but I found exodus to be much faster than JAXX. Exodus can be backed up and the security features are also good enough even though it's a hot wallet. Exodus also has a built-in exchange between the cryptocurrencies that it supports but same as JAXX, you must have some of the coins beforehand transferred onto your Exodus wallet. For example once you send some bitcoins to your Exodus wallet, you can exchange them to any other cryptocurrency which Exodus holds. The interface is very user friendly, anyone you can download it for free and there is no registration required. Exodus is continuously adding additional cryptocurrency wallets and it's still very fast.

Chapter 17 TREZOR

In this chapter, I will talk about the Trezor Wallet. Trezor is a hardware wallet, which is currently one of the best in terms of security. Trezor is an excellent cold wallet that provides cold storage to store your bitcoins or other cryptocurrencies. Once you have a Trezor, you will know why it is so secured. It's screen has limited visibility to the end-user offline. Meaning, the Trezor screen is not visible on your computer; therefore, hackers can't get to it. Your private keys are also completely offline. The interface is very easy to use and I would recommend it to anybody. The Trezor also has a web interface; but the screen is built in to provide additional security. Trezor is an open source wallet, therefore, in case you lose it you can buy another one or similar device that supports the same functions and you can back it up very quickly using the recovery seed. At the time I bought it back in 2015 was 79 Euros but I also purchased a cable for an Android phone and paid for DHL shipping which costs me a further 26 Euros. When I was about to make a payment, I also got billed for 21% VAT so instead of 79 Euros I ended up paying 135.20 Euros. They are scammers but you will get charged for postage no matter where you order from and the VAT itself was 25.2 Euros. Trezor is produced in the Czech Republic and if you reside in the country you might not require paying the VAT. Trezor is not a scam and it is a must have wallet but before you consider buying one make sure that you are aware of the additional charges. Something else you should consider is the waiting time. When I purchased the Trezor wallet there was a warning message on their official website that it would take six weeks for delivery. But once you click on ok and click on payments, you have options for DHL delivery that is between 3 to 5 days costing 26 euros, or traditional delivery that takes between 4-8 weeks for 12 Euros. I ticked DHL delivery as I wanted to store all my bitcoins on a secure wallet as soon as possible. Still, after six working days passed, I send them an email to find out where the wallet is. They replied that, there is a warning message about the delivery which states that the delivery takes at least six weeks,, I didn't understand at the time if it takes six weeks to deliver the device then why do they still offer 3 to 5 days DHL delivery. As a result I sent another e-mail to find out an answer and got a reply that after 6 weeks once the Trezor is back in stock the delivery will be only take between 2 to 5 days instead of 4-8 weeks. So, in the end I got it

after five weeks but it is a long time to wait. In the other hand Trezor is a must have wallet, so it's ok and it was worth to wait for it. While I was waiting for the wallet to arrive, I had some bitcoins on my Blockchain.info wallet which didn't get hacked or anything like that but when I have received my hardware wallet I have moved my funds right away to my Trezor. At the time I purchased the Trezor it supported only Bitcoin, Bitcoin cash, Litecoin, Dash, Ethereum, Ethereum Classic, zCash, Nem, omiseGo, civic and Golem. But as of 2020 November, the Trezor wallet supports 1631 coins and tokens. To find a full list of cryptocurrencies that Trezor supports, please visit https://trezor.io/coins/

When you set it up you will need a Chrome extension which you can download to Windows, Mac or Linux machines too. When you visit their website at https://wallet.trezor.io/#/ you can click on start now where you can learn how to set up your pin code and how to record your recovery phrase. Next you should click on Docs and navigate to Trezor User Manual and here you can find everything there is to know about the Trezor wallet. What's in the box, how to setup the device, how to receive payments, how to make a payment, recovery, emergency situations, security best practices, two factor authentication and so on. Basically once you have a Trezor wallet you should really allocate at least 1 maybe 2 hours to fully understand all the features because once you have a hardware wallet like Trezor, YOU ARE THE BANK! As a result, you will have responsibilities so you need to know how things functioning. I must have taken 3-4 hours to go through all the features that Trezor have. As I mentioned before to set up a hot wallet is easy but they do not come with great security. Another tip I can recommend is to make sure that you don't rush it and while you do your setup at the first time, you really don't want to be disturbed half way in the process. You should try to allocate at least 3 hours for this purpose. You can buy the Trezor from their website at https://shop.trezor.io/

The current options you have are Trezor One which is now only costs 58,51 Euros. This comes in either white or black. Then you can have the Trezor One Metallic which is 600 Euros. And lastly you can purchase their latest device called Trezor Model T for 178.8 Euros.

You might also check out the closest Amazon to you and see the price there first as Amazon provides faster delivery in most places especially if you have Amazon Prime. There are 13 different Amazon shop out there. There is

Amazon US OR Amazon.com but if you are in Europe you might check out Amazon.co.uk, Amazon.de, Amazon.it, Amazon.fr or Amazon.es and see which one is delivering to your Country. There is also Amazon.in Amazon.ca, Amazon.mx, Amazon.co.jp, Amazon.com.br and Amazon.com.au. One thing you have to look out for is that Amazon is pretty much always out of stock. Also if you do find one on Amazon, you might see that is more expensive and this is because resellers are selling for a higher price range which might be ok considering if Amazon has stock, they will deliver you to within a day or two. In the next chapter I will explain the key differences between Trezor One and Trezor Model T in more depth.

Chapter 18 Trezor One Versus Trezor Model T

The Trezor One and Trezor Model T are both designed by the company called SatoshiLabs. Both are famous for their usability, security and support for a wide range of cryptocurrencies. The Model T is the later version; it has more features and is more expensive than the old version called Trezor One. The Trezor Model T supports more cryptocurrencies, it also has a new touchscreen and new hardware features such as an SD card slot and built in mobile connectivity. When choosing a hardware wallet, the first thing you can check is whether the specific wallet supports those cryptocurrencies that you have already invested or planning to invest in the future. The Model T backs all the cryptocurrencies that the Trezor One supports and much more. Both the Model T and One support most of the major cryptocurrencies and all of the ERC20 tokens. SatoshiLabs and other third party wallet developers are continuously adding support for more cryptocurrencies on both Trezor wallets. If you are a crypto investor especially interested in purchasing diverse altcoins or alternative coins, you can purchase them online but once you do, make sure that you store them securely offline in your hardware wallet and Trezor is just what you need. But which one should you get correct? Well, the most notable difference between the Trezor models is that the Model T has a touchscreen and the Trezor One has the old “two push buttons”. The touchscreen’s main advantage is accessibility; however it also provides a security advantage during the recovery seed process. With the Model T you can simply enter in a recovery phrase exclusively through the device’s touchscreen. This look after your recovery seed from being entered in on your workstation and possibly being compromised by Malware containing key loggers. The touchscreen is more accessible than the two push buttons. Not only entering recovery seeds easier and more secure, but also entering passphrases, PIN codes and configurations for the actual device. The touchscreen is also a large display which makes it easier to see and verify the public address during any transactions. The hardware of the Model T has been advanced for the next generation and it has a USB-C connector and a MicroSD card slot too. The device also has a faster processor and operating system and the USB-C connector is compatible with any workstation or android device. The MicroSD features are not yet practical but SatoshiLabs plans to use the card slot for data encryption, password management and

signing offline transactions as well. Therefore as you can see the Model T was built with expandability in mind. Both wallets offer the same sophisticated security and if used correctly should protect you from any type of hacking. Both wallets features PIN Code, Cold Storage, Advanced Passphrase, Password Manager and U2F, Native support for ERC20 tokens, Address Verification and Recovery Seed. They both allow native support for ERC20 Tokens which means that you can use the Trezor web wallet interface to send and receive ERC20 Tokens instead of third party interfaces such as “MyCryptoWallet” or “MyEtherWallet”. Trezor wallets utilise hierarchical deterministic recovery seeds which is a method that secures all your private and public keys and addresses with a 12, 18 or even a 24 word recovery seed. You can then write down this recovery seed on paper and store it completely offline. If the Trezor physical device is lost or stolen, you will be able to recover all of your assets by entering the recovery seed into another Trezor wallet or into any other compatible wallet. Both the Model T and the Trezor One generates a 24 word recovery seed but can also take in a 12, 18 or 24 word recovery seed from other compatible hardware wallets. The Trezor Model T only needs 12 words as opposed to the Trezor One because the recovery seed of the Model T is exclusively entered on the touchscreen and not on your workstation. If you have a 24 word seed that you were using with a Trezor One, then you will be able to import that recovery seed and all of the associated cryptocurrencies onto the Model T. If an illicit person gets access to your wallet, they will still not be able to gain access to your assets because of the PIN Code. The PIN code is 4-9 digits long and gets reset after multiple failed attempts. If you forget your PIN Code, you can reset the device and recover all of your funds with the recovery seed. Once you are sending or receiving cryptocurrencies, you will confirm the address on the screen of the wallet. This protects you from accidentally entering in the wrong address and from malware that can changes the address in the last second. The address is easier to read on the Model T because of the larger screen. Both wallets can be used as password managers and two factor authentication devices aka U2F too. Nowadays it can be difficult to remember all the various complex passwords for each of your online accounts but the Model T can remember all your logins, URL-s and password information. Once you are logging into an account, you can confirm on your device and it will enter your password in for you. The feature called “Trezor Password Manager” works with Google Drive or Dropbox to store passwords in an encrypted form. If your

device gets lost or stolen, you can still recover all of your password information with your recovery seed. Both Trezor wallets also have the option to serve as a two factor authentication device for any of your online accounts. Two factor authentication is when you use a device to confirm your login, in addition to your password and username. The Trezor wallet uses Universal Second Factor authentication which is a greater technique than the commonly used Time-based One-time Password (TOTP) authentication. In summary both devices have their pros and cons and if you are about to start investing in cryptocurrencies while you don’t want to spend too much on a hardware wallet, you might go for the traditional Trezor One device. I personally did not upgrade to Trezor Model T yet and my Trezor One is over 4 years old and still functioning just fine. But if you are planning to invest tens of thousands of dollars into cryptocurrencies and want to keep them in a safe place, you might choose to go for the Trezor Model T.

Chapter 19 How to setup the Trezor Model T

Before we get started, I would like to point out that if you do get a Trezor Model T, you should also try to get a long extension cable because the default cable is very short and it doesn't give you a lot of wiggle room to maneuver when you're on your computer. Assuming if you can afford the Trezor Model T for $180, you should also be able to get a one meter long extension cable for another $7.99.

Once you have a device it comes with a small extension cable to attach it to your computer. It also comes with two copies of recovery seeds which you should guard with your life because this is everything if your device stops working or gets stolen. If your device stops working this recovery seed will allow you to get back all of your funds on a new device.

For the first time when you try to turn on the device you have to take the cable that comes with your device and plug it into the bottom and just plug it in the other side of the USB into your computer. When you do so, you'll see a "welcome" on the device's screen. At this point, you should go to https://trezor.io/ on your web browser and then go to "wallet" then select "Trezor Model T" where you will see a screen saying: "Before you start" followed by a message saying that you should make sure that the hologram seal on your device is authentic. If the hologram seal is missing or looks differently from what they represent on their website, you should contact immediately the Trezor support team. They will get back to you but in the meanwhile it is not recommended to use the device. So if the sticker or the hologram seal on your device is authentic, you have to remove it and plug it in. Next, click on "continue to wallet" and now it's going to tell you that "it's time to install the device firmware" so select "install firmware" and you'll see the installing on the screen and you'll also see it installing on the device. This shouldn't take very long, maybe about 15 to 20 seconds and now it's going to reboot and when it does it will move on to the next phase of the installation.

Here, you will have to clock on "create wallet" and then select "create with single backup". On your device it's going to ask you "would you really like to create a new device" so you're going to have to select the check mark. Next, your device is going to say: "we need to make a backup" and in the meanwhile you will see on your computer screen a message "Preparing your

Trezor”

So next on the screen you will see if the message saying “your trezor is not backed up” and you will see an option for “create a backup in 3 minutes” so click on that. Once selected, click on “continue” and now your device screen will say “don't make a digital copy of your recovery seed”. This is why they give you the recovery seeds or pieces of papers so you can use those to write down your recovery phrases. In a nutshell, you can be hacked if you take a picture of your recovery seed or if you send an email to yourself having the phrases inside the email or if you save them on your computer, there's always the possibility that your computer gets compromised and you can lose all the funds that your device holds. So once again, never take a digital copy of your recovery seed. Moving on, at this point on the bottom of your device will say “I understand” so you have to click on that. And now the twelve words that are your recovery seeds will pop up on your device. For security reasons do not show this to anyone, but at this time make sure that you write down all those twelve words. After you write down all twelve of your recovery words, it's going to ask you to confirm that you have written them down in order. It will ask you for three of them which you have to confirm. In the meanwhile your computer screen will have a popup message saying “Complete the action on your Trezor device” so you can’t really do anything until you have finished confirming your recovery phrases. Once completed, your device will say “you've done verifying” so click on “done” while you will see your computer moving to the next stage saying “you have successfully backed up your device!” and you can click on “continue”.

Once successfully backed up your device, keep your recovery seed in a safe place so if anytime you need to recover your device, you have your recovery seed written down. Once on the next page, your computer screen will say “enter a new pin for my Trezor” and there is another message saying “Complete the action on your Trezor device” so once again, you have to do this on the device instead of the computer. This pin number will be important because every time you log into your device or you plug it to the computer, it's going to ask you to put in your PIN first. This is for added security. At this point your Trezor device will ask you if you really want to create a new pin and you have to select “yes” then it will ask you to enter a new pin.

So here you have to enter a new PIN and if you might think that will forget this pin number in the future, maybe it is better for you to write this down

too. Once complete, your device will say “you have successfully created a pin number” so then select “continue”. At this time your computer screen will “Good job! Your PIN is set,” so click on “continue” At this point you have to name your device for example Boris’s Trezor T” then click on “confirm to continue”. Here, your computer screen will say “Confirm action on your Trezor device” so once again, you can’t continue until you confirm the new name of your device on your Trezor hardware wallet. Your device will ask you if you really want to have a new name for your device, so you have to select “yes”. Once selected “yes” on your device, you will see that your computer will take you to the next page where you will have a message saying “you choose a wonderful name!” which is funny from the Development team, but here you also have to click on “continue”

Once selected, the next page will offer you to bookmark this page in your browser by using a shortcut of Ctrl+D and then clock on “done” and then click on “continue”. This option might be overlooked by many people or thinking why would you need this, but this is not an optional. This is good in terms of security because it will always take you to the Trezor’s website. There' phishing attempts from hackers online trying to get your funds so that's the safest way to do it. Moving on, once you have selected “continue” it will ask you for your email address to stay in touch but this is optional. You don’t have to give them your email address of course but if there are updates available to your device you want to be informed so even if you don’t want to give Trezor your personal email address, I would recommend to give them your secondary email so you stay informed if upgrades required in future.

At this stage you can either click on “skip this step” or “continue” on the next page you have to click on “Finish” and that's it! Your device is now ready to run! Your device is all set up. If I want to receive bitcoin, you just click on the “receive” tab where you will see that your public address is greyed out. What you want to do to access the full address is click on the option “show full address” and in the meanwhile your device is also going to prompt you and it's going to show you the exact same address as your computer. As a reminder, this is ok, as this is your public address and if you want anyone to send you bitcoins or other cryptocurrencies, this is the address you want to share with them. So here, your device will ask you to confirm that the address on the device is exactly the same what your computer screen shows you. Once again this is another security feature to make sure you haven’t done

anything wrong.

Once you have visually confirmed that on both screens of your device and on your computer the public address is the same, you also have to confirm on your Trezor device. At this point you'll have full access to this public address so once you receive bitcoins on this address, this address will change of course. Public addresses receive a fresh address every single time you receive bitcoins to them using digital signatures. This is just another thing that no one seems to talk about, but if you keep on receiving bitcoins for example and each time you want to give someone your public address, you will see that your address is always different until you receive another transaction. Additionally, you can set up multiple accounts if you'd like for example you want to have one account for personal usage and another account for your business, you could just click on “Add Account” and you can have multiple accounts. Once thing you should know is that if you want to create another account, the previous account must have some transactions. If you have followed this guide step-by-step, your device should be successfully setup and ready to send or receive bitcoins or other cryptocurrencies.

Chapter 20 How to setup KeepKey

In this chapter, I am going to talk about the KeepKey hardware wallet. KeepKey is another hardware wallet that you can buy which supports Bitcoin, Bitcoin cash, Ethereum, Litecoin, Dogecoin, Dash, Cosmos DigiByte and XRP. KeepKey also supports ERC-20 tokens such as AELF, Aeterenity, Aragon, Augur, Balancer, Binance Coin, Bancor, Chainlink, Civic, Compound, Dai, FOX Token, Golem, ICONOMI, Metal, OmiseGO, REP and SALT just to name a few. KeepKey wallet is produced by the company called Shapeshift and you can buy it from them by visiting their website at https://shapeshift.com/keepkey

They only have one colour or one version of KeepKey hardware wallet which is currently costs 49 dollars. KeepKey works in conjunction with the wallet software on your workstation by taking over the management of private key generation, private key storage and transaction signing. With KeepKey, your private keys are generated on the device and never touch the internet. KeepKey's cutting-edge technology also lets you to safely access your cryptocurrencies on an infected computer without compromising your security or peace of mind. KeepKey communicates with a connected computer using a limited protocol and KeepKey never reveals its private key. This limited protocol only allows for transaction requests, which must be manually approved using the device's confirmation button before KeepKey will sign it. KeepKey is more popular in the US then in Europe. You might look for one on Amazon.com and check out the price there because I have seen it before for $29. They might be running a promotion or even resellers often buy them in bulk and sell them cheaper. KeepKey has a very large screen which is useful for viewing public keys and verifying transactions. Once you have a KeepKey, first you most probably have to update your device. Once plug it in to your computer or MAC, you will get a prompt for the KeepKey updater. Once you click on it, you have to allow it to run the updates. Next when the updater is complete, it will prompts you to update the firmware and the boot loader. After that, it will ask you if it's a new device or backing up a device. While the update is happening, it will prompt you to push and hold the device button until you get a confirmation to release it. Next it will prompt you to unplug then plug back in the device. Once complete, you will get a message on your screen that the updates complete

and you should click on go to ShapeShift website to pair your device. Here, you have to click on “Pair your KeepKey”. Here, you will have to label your device, basically you have to name it for example “Boris’s KeepKey” then click on “set label”.

Next, it will ask you to create your own pin number. While you do this step, the numbers will not be shown on your computer screen. But they will be seen on the KeepKey device, even though you have to click the corresponding tale on the computer screen which is representing number that you want to have for your device. You also must know that each time when you plug in your device the numbers are always scrambled. Therefore the combination you see on your computer screen will not be the same combinations what you enter each and every time. The next step will be your recovery phrase generation. Basically you have to generate your own backup phrase which you have to record on a piece of paper. It is always best practices that you do not share those keys with anyone else and do not keep a digital record of it. Your backup phrase is also known as your recovery phrase which are 12 random words in the case of KeepKey hardware wallet. Those private keys are only visible on the device which is great so hackers can’t see that or can’t access it from the internet. Then you have to download a Google chrome extension so you can access the wallet from the computer using a web application. Regards to KeepKey, you can also buy bitcoins or other cryptocurrencies as you can integrate the wallet with Shapeshift’s platform. In terms of sending or receiving bitcoins, the confirmation must be done manually on the device, so because of that reason I do recommend to anyone who doesn’t want to spend too much for a hardware wallet.

Chapter 21 Ledger Nano

In this chapter, I am going to talk about the Ledger Nano hardware wallet. This is also one of the best hardware wallets I can recommend. There are many software wallets you can use for free of costs right away and you probably should as your first wallet. However, when it comes to investing especially large funds, hot wallets are not safe. Therefore, I would only recommend a low amount like 100 dollars as your first investment on hot wallets. Anything less than 500 dollars is not that attractive for Hackers, but it doesn't mean that your funds are safe on hot wallets. Therefore, only invest as much as you are not afraid ready to lose in case you do get hacked or lose your private keys. So, to visit the Ledger Nano's website, go to https://www.ledger.com/

Once on the side, click on Crypto assets, and then you will see all the cryptocurrencies that the Ledger Nano supports. The Ledger Nano supports Bitcoin, Bitcoin cash, Monero, Bitcoin gold, Ethereum, Ethereum classic, Litecoin, Dogecoin, Zcash, XRP, Dash, Stratis, Komodo, Ark, Expanse, UBIQ, Vertcoin, Viacoin, Neo, Stealthcoin, Stellar, H-cash, Digibyte, Qtom, Pivx and so on. There are many great cryptocurrencies that the Ledger supports while some of them are completely useless. There are many reasons why I recommend Ledger Nano as one of best hardware wallets. For example, if you look at any of these coins that the Ledger supports, you will find that they are also providing additional documentations for each and every token or cryptocurrency. For example if you look at Bitcoin documentation, it explains how to access, configure and troubleshoot the Bitcoin chrome application. If you click on it you have the table of contents and you can see that they have a tutorial on everything. There are other very useful tutorials too like HOW TO BUY BITCOINS which explains step by step what you need to do but you can also submit requests or you can see related articles. There are also recently viewed articles and many of the tutorials have comments too. If you go back to their main page and click on "chapters" then select the device which you want to see on more chapters for, you can find various how to guides. For example how to configure a new device, how to navigate the dashboard, how to send bitcoins, how to restore a configuration, how to reset the device, how to send ethers, so you have everything there is to know about the device which is really helpful. To buy a

Ledger Nano, you have to click on “products” and choose which device you want to review or you can simply select “compare our devices” where you can see side-by-side both their products called Ledger Nano S and Ledger Nano X. The current market price for these devices are $69 for the Nano S and $119 for the Nano X. The Nano S is their best seller, which is also their first product came to the market back in 2014.

My recommendation is to go for a Nano S and if you want to buy it just click on “add to cart” and check the shipping schedule as you might find that they only can deliver within 2 months which is long time but the demand for these devices are extremely high. Next if you click on “add to cart”, then “checkout”, when you scroll down to payment method, you can see that they also accept bitcoins for payment which is great. In my case Ledger Nano S was no different than Trezor when it comes to delivery. I had to wait nearly 6 weeks for the device to arrive. Back then when I bought the ledger it was also cheaper. The difference was that the Ledger Nano S was only 59 Euro which already included VAT. I had to pay for the postage fee another 16 Euros for UPS delivery which totalled a full payment of 75 Euros. A few months later I have ordered another Nano S for back up as my saving account but Due to a very high level of demand I have only received that within 8 weeks from the order date. The ledger company is based in Paris, France so it depends which country you reside you might get it earlier than I did at the time. If you do not want to wait for weeks you can check out Amazon and see if they have in stock but it will probably more expensive. Back at the time when I was ready to buy a hardware wallet I tried to buy it on Amazon even if the device was more expensive, still Amazon was out of stock. If you are in a rush and just want to use a Hardware wallet right away, I would advise you to check Amazon first as you may get it a lot faster — if they have it in stock of course.

When it comes to the build quality, the Ledger Nano is what I would recommend as it has durability which able to take the weight of a car. The Ledger company not only claims this but my friend tested if it’s true with his Fiat which he filmed and showed me, so I have seen that is indeed very strong. My final recommendation is that you definitely have to have a cold wallet so you cannot be hacked and the Ledger Nano S is just perfect for this purpose. When purchasing the Nano from their website they don’t add additional VAT fees to the price and I think it also looks much better. It’s a

personal preference really. The Nano S is cheaper than Nano X or the Trezor, while it is more expensive than KeepKey.

Chapter 22 How to setup Ledger Nano S

If you choose to have a the Leger Nano S or you already have the device and want to set it up at the first time, this guide will help you just do that. First of all please visit https://www.ledger.com/start where you will see four different steps.

Step 1 is called: “Get Ledger Live to start setting up your device”

Step 2 is called: “Choose a PIN code & write down your recovery phrase”

Step 3 is called: “Install applications on your device”

Step 4 is called: “Add an account to manage your crypto”

So in a nutshell, you're going to download the ledger live app, you're going to create your pin and get your recovery phrase, you're also going to install the applications on your ledger and then add an account to manage your crypto. That's what it is in its plainness. Once you click on “download ledger live app” you will see the options for Windows, Mac, Linux, App Store and Play Store. Once you have selected the right operating system, click on “download app”

Once downloaded the app, you can move over to step two and plug in your device using the USB cable. Once plugged in, you will see a “welcome to ledger nano” on your device screen. On the device facing yourself you will see two buttons on the top of it, one on the left and the other on the right. You're going to have to push both buttons at the same time to confirm your selection. But first, you have to push the one on the right to see the menu options or push the left button to go view the previous menu option you just viewed. You will see a few options and once you see “set up as a new device” you have to push both buttons to validate it. If you keep on pushing the right or left buttons on the device it will show you further options such as “restore from recovery phrase” which is not what you are after so carry on pushing the right/left button until you get to the menu option called “set up as a new device” and push both buttons to select this menu option. Next, your device screen will say “Choose PIN code” so once again push both buttons to select this menu option. Once at this stage, you have to create your pin code then what the device will ask you to confirm the pin code again to verify it. Once complete, the device will say “Write down your recovery phrase”. Here

you will have only one option which it to push the button on the right which will show you the first recovery phrase that you have to write down.

You have to do this step 24 times to see on your device all your recovery phrases so you can write them all down to the piece of paper called Recovery Sheet. Then after you get through all 24 words, you're going to see the next message on the device saying “press left to verify your words”. Once selected, it will say “confirm your recovery phrase”. At this time you have to select both buttons at the same time to confirm, which will prompt you to “confirm word one” and then it's going to go through all 24 words for which you have to confirm then you will move on to the next phase.

Once you have verified all 24 words which are your only backup you have to keep them in a secure place and should never share them with anyone. At this stage the device will say “press both buttons to continue” and now it will process your device. Next, you will see on the device “your device is now ready” where you will have an option to push the right button only, then it will say “press both buttons to enter dashboard”.

Once complete, you are inside the Ledger as a newly set up device where you can navigate within the menu options until you find the menu called “install app” then select “Open ledger live to install apps”. If you want to see what other options you have you can carry oh navigating left or right where you can see options such as “settings” where you will see additional options like “display” where you can change your display settings. There is also an option called “security” or “firmware” where you can see the firmware version or if you want to “change your PIN” your “passphrase” or “reset all”. You can practice with it to see how it works. For example you select “reset all” on your device it will allow you to recreate a new fresh ledger.

These are other options that you should be aware but to finish setting up your device, you have to choose “press both buttons to enter dashboard”.

Once you are on ledger live on your computer screen, you will see the message saying “Welcome to Ledger Live” where you can select application to run on light, dusk or dark mode. Once selected, click on “get started” then choose “set up as new device”. Next you have to select what device you have and in this case we have the Nano S and click on “continue”.

The next page will say “security checklist” where you will see the following questions;

“1. Did you choose your pin code by yourself?”

“2. Did you save your recovery phrase by yourself?

“3. Is your ledger device genuine?”

For each of these questions you can select an answer as yes or no. When you are answering to question number 3 called “Is your ledger device genuine?” it will prompt you to check now and will ask you to “connect and unlock your device”. At this time you have to put your pin into your device then push both buttons to allow the ledger manager on your device.

Once complete you should see the message saying “Device is genuine” then click “continue”. The next page is called “password lock” which is optional but here you can set a password to prevent unauthorized access to Ledger Live data on your computer, including account names, transactions and public addresses.

After selected and confirmed a password, the next page will say: “Bugs and analytics”. This is where you can select what you want with analytics and bug reports if you wish to share information with Ledger company so helps them fixing bugs but it’s optional, so once ready to move on just select “continue”.

The next page will say “your device is ready!” and you will see an option called “open ledger live”. Once clicked on it, you will see your platform menu options on the right called “portfolio”, “Accounts”, “Send”, “receive”, Manager” and “buy crypto”.

If you click on the option called “portfolio” you will be prompted to “allow ledger manager on your device” meaning you have to push both buttons on your Nano device to access your portfolio.

Once have done it, Ledger live will recognize your Ledger Nano S and you will see additional information which you haven’t seen until now.

You will see the firmware version number, how much space is used and what is the total capacity of the device, an option for “app catalog” and “apps installed”.

Within the option for “app catalog” you will see many cryptocurrencies where next to each you will see another option called “Install” which you have to click on to get a wallet. Once the installation is complete you will see

“installed” however each time you install a new cryptocurrency wallet, you have to keep on eye how much space you have sued on the hardware. You don’t have to worry too much about these as you will see how much space each cryptocurrency wallet takes while you can also see how much space you have left. In average you can get between 3 to 6 wallets for the ledger Nano S.

As an example let’s say that you have downloaded the Bitcoin app, the next thing you have to do is to add a Bitcoin account. To do that, you have to click on “add account” then click on “continue”. At this stage you will be prompted to confirm it on your device by pushing both buttons at the same time. Next, you will see that is synchronising and once confirmed you have to click on “close”. You can download and add accounts to other cryptocurrencies too following the very same process. There are many features that the Ledger Nano is also capable but that is it in a nutshell. Your Ledger Nano S is ready to receive or send bitcoins or other cryptocurrencies.

Chapter 23 How to setup the Ledger Nano X

Nano X is the latest product from Ledger and it has a number of upgrades from the older model called Nano S. The main upgrades are the larger digital display and the two buttons on the front rather than on the top. It's a little more sturdy and a bit heavier but the actual number of applications that you can install is greatly increased. The old legend used to get full with three or four applications wallets and that's not very good if you've got lots of different cryptocurrencies. The Nano X can fit over a hundred applications so discuss how to set all this up. First of all, make sure that you've purchased one off the official web site and you don't buy a second hand device as there are plenty of scammers out there trying to take advantage of you. Also make sure that it comes in its original packaging when you get it. You can connect the Nano X to your computer but it does have Bluetooth enabled feature too. The first thing you have to do is download and install the ledger live up from the site called https://www.ledger.com/ledger-live/download

Once there, click on “Download” and choose your operating system you want to use the Ledger Live App. On the official Ledger website explains that you can actually get the ledger live app on your phone and then pair it with Bluetooth and use it that way too but I still think the best way to set it up on your computer is to use the cable or at least the first time. Once you have downloaded the Ledger Live App, just open it and click on “get started”. This is where you can restore it from an old device if you've written down your backup phrases. If you've the backup phrases stored safely and you lose your ledger, or it breaks for whatever reason or you just want to import your old ledger information on to the new device this is where you can restore it at this point. But I will explain how to set it up for the first time. So once you clicked on “get started” you will have the following options; “Initialize as a new device”, “Restore device from recovery phrase” and “Use an initialized device”. Here you want to click on “Initialize as a new device”. Next, you will have to select “Ledger Nano X” and click on “continue”. The next page will ask you to go over to your device and start to set up a PIN number. On your Nano X you can use the right or left button to different digits and hold down both buttons to confirm your pin numbers. As a new device it's going to ask you to choose a four or eight digit PIN number so once you select that please remember that you never share that information with anyone. Once

completed, you have to confirm the pin number for the second time and it’s going to ask you to write down your recovery phrase. This step is really important that you write them down in the correct order all those 24 words. This is the most important thing because this is your final backup. If something goes wrong and you lose your ledger, to restore all your cryptocurrencies you must have these 24 words. Once you have written down those 24 words in order on to your recovery sheet, it's just going to ask you to confirm them again. This is going to take a little while so make sure that you don’t rush it and don’t make mistakes. Once you have re-entered those 24 words, the device is going to say “processing” followed by saying “completed correctly”. Once completed, you want to head back to the Ledger Live App and click on “continue”. The next page will ask you if you have written down your recovery phrase, and here you can just click on “yes”. Next page will ask “did you choose your PIN number yourself” and “did you save your recovery phrase” so click “yes” on both. Then question 23 will ask “Is your Ledger device genuine?” and here you have to click on “check now”. This will double-check you've done everything so far properly and then going to tell you that “your device is genuine”. Once the security check is completed, click on “continue”.

The next page is just an optional set up called “Password lock” which is another layer of security. This isn't for the actual Nano X device but rather is another layer of security on your computer or on your phone. You can add another password there, and then click on “continue”. Next page is where you have the “bug reports and analytics” which you can choose to participate but it’s also optional, so once selected your preferences you can click on “continue”. The next page will say “your device is ready” and you will have an option called “open Ledger Live” so click on that. On the next page you have to click on the menu option called “open manager”. This is so that you can install the app and then once you have installed the app you can add an account. To start off with the first installation, you can choose the Bitcoin app and click on “install”.

This is for downloading an app onto your phone or laptop but once you downloaded the app you need to add an account to it which is an address for your Bitcoin. Just because you have the app it doesn't mean that you have actually got an account setup too so this is a 2-step process which confuses a lot of people. Once you have installed the Bitcoin App, you can install many

more cryptocurrency apps as the Nano X has much more space then Nano S. Additionally when you download cryptocurrency applications you will also see that the Nano X is much faster than the Nano S. Once you have installed all the apps you wanted to have an address, you have to head over to “accounts” and you have to add an account. For example you have installed the Bitcoin app, now you want to create a Bitcoin account for it. So if you type “Bitcoin” in the required field, then choose the asset you want, it's going to ask you to navigate to your Bitcoin app on the digital display and then click on both buttons. Next, click on “continue” and it's going to sync up. This shouldn't take too long but the first time you do it, it will take a little bit longer than when you revisit it a second time. This is setting up a Bitcoin account for you and an address. Next you will see that you have “successfully added a Bitcoin account”. As an example, if you try and add a litecoin account for example, it's not going to let you add an point account because you haven't installed the litecoin app yet through the manager in the ledger live. So if you want to add additional account for other cryptocurrencies, you must first install those applications. Once you have created an account in ledger live manager you can is click on “Bitcoin” for example and click on “receive”. This will ask you to go into the Bitcoin app and press both buttons on your device. Once this opens up, it's just going to ask you to verify the address on our device so click on “continue”. This is going to pop up your Bitcoin address on your computer screen and it's going to have the same address on the display screen of your Nano X as well. If you're new to all this and you've just bought some cryptocurrency for the first time this is the address that you want to send your bitcoins. It can be safely stored on your device rather than the exchange. You can copy this and then you can paste it for example to the exchange or wherever you are sending your bitcoins from. The process is the same with any other cryptocurrencies too. Just go into the manager, install more apps and then you create an account. Those account then you can call them anything you want with the different cryptocurrency wallets and then you generate those address to store them safely. Hopefully that's a good and easy explanation. In the next chapter I will explain how you can update the firmware for your Ledger Nano.

Chapter 24 How to upgrade the Ledger Nano Firmware

In this chapter I will explain how you can update your Ledger Nano whether it's an S or an X. I know some people got really scared when they installed the latest updates then suddenly realized that their bitcoins have been missing from their hardware wallet. But as it turns out they forgot to reinstall the apps and their associated account back to the wallet. So to avoid confusion let's walk through the firmware upgrade process step by step. First you have to open up Ledger Live, and once is up, you will see a message on the top of your scree saying "ledger live 2.9.0 is available for update" and you will see on the side "Download now". Once you click on "Download now" it will start downloading the latest software and once complete, you will a message saying "Update ready to install" and on the side it will say "install now". Once click on "install now" it will reset itself so you will have to put your password in again and it will have a new pop up window called "release notes". This will list the new features and recent bug fixes which you can read then you have to click on "continue". Update is now complete but if you want to verify it you have to click on "settings" and then click on "about" where you will see the Version number. Here you should click on "Details" to confirm that you have the latest version installed. Then you also want to check your Nano S or Nano X which you have to plug in then go to "manager".

You also have to put in your pin code to unlock your device then once you get into the manager section of your Nano x you will see 1.2.4-1 as the firmware on your ledger Nano. You might see a different version at the time of reading this book and you should also see on the top of your screen that "firmware version 1.2.4-2 is available" and on the side you will have an option called "update firmware". To update that firmware you have to click on that which will bring up another popup window for the firmware upgrade details but here you will also have a warning for you saying "I have my recovery phrase". You have to tick that box and then click on "continue".

Next, it will take a few minutes to complete the upgrade so you have to be patient. Before the download window would reach 100% for completion, your Nano is going to ask you to confirm a special code physically on the device, so you have to confirm that first. Once confirmed, you will see on your computer screen a message saying "device in Bootloader mode. Click

on Continue to update it.” Here, you have to click on “continue” and in the meanwhile your Nano will say “boot loader mode”. It is very important that this point you must not disconnect your device because you can easily mess up the whole firmware update. Once complete, you will see that is says “firmware updated please reinstall the apps on your device”. This time you have to unlock your Nano and put in the pin code. Next you have to click “install” on the Bitcoin apps or any apps that you had before on your Nano. Once the apps are installed, go to “manage my accounts” and you have to click on “add an account” then select Bitcoin or any other account you had before in a similar fashion as you would set up your device the first time. It's pretty self-explanatory you just select continue, update, add your pin code make sure you put that in correctly and you're good to go. From there, always keep your recovery phrase backed up like i said before, you use those cards that you get with your Nano and keep those safe. Keep those hidden so you can pull them out and make sure that everything is correct on your Nano. You never want to lose those recovery phrases because then you can lose your crypto assets. Also if the firmware upgrade goes bad, Ledger will be happy to give you hardware but if you don’t have your recovery phrases you will lose access to your cryptocurrencies. Therefore always keep that in mind you are your own bank and you must double-check and verify everything to make sure it is all safe.

Chapter 25 Additional Hardware wallets

In this chapter I will talk about additional hardware wallets starting with the Ledger Blue. The Ledger Blue is one of the largest hardware wallets available on the market. It was designed with accessibility in mind, permitting individuals and businesses with limited cryptocurrency experience to safely store their investments. Like all other Ledger wallets, the Blue features top-notch security that has never been hacked. While the device's large touch screen makes it simple to use, its poor availability and limited asset support make this wallet only suitable for those that prioritize ease above everything else.

NGRAVE

The next on my list is called NGRAVE. The NGRAVE is a new competitor to the market. The device doesn't allow you to connect to the internet in any way. Instead it's using a USB port or Bluetooth communication to relay information to connected devices while is completely offline. This means that you will never have to worry about compromised software. Another great feature is that the NGRAVE device also comes with an Everlasting Backup for your seed recovery. These stainless steel sheets are fire-resistant and water-resistant. This makes storing your seed code easy compared to other wallet providers that only include a piece of paper to backup your recovery phrase. The NGRAVE has a unique design and it cannot be compromised digitally so you never have to worry if your hardware wallet's software requires firmware upgrade or not. This is good for people who want complete peace of mind about their cryptocurrencies especially for those that travel often with their hardware wallets. The NGRAVE also includes a stainless sheets right out of the box to simplify the proper storage of your seed phrase. The only issue is that the device is manufactured by a new company and the community support may take some time to be as good as the Trezor or Ledger Company.

BitBox02

Next on my list is another hardware wallet called BitBox02. The BitBox02 is

a nice tool for individuals to easily store, protect and transfer their cryptocurrencies. It comes with the BitBoxApp which provides the management for your digital assets. The BitBox02 looks like a small USB-C thumb drive and the display is not visible when it is turned off. Because the device has no visible screen when turned off, the BitBox02 is a very discreet wallet. The wallet comes with a USB adapter, a USB extension cable and a microSD card for the backup. You can also get additional MicroSD cards for backup redundancy if you require. According to the manufacturers, the hardware wallets has been available since 2016 and have been sold in various countries, but personally I only heard about it in 2019 for the first time. The BitBoxApp has an easy connection to your own Bitcoin full node if you are a miner. The wallet also compatible with MyEtherwallet, therefore power-users can utilise their favourite tools with added hardware security. The device uses a secure chip for physical device hardening in combination with fully open-source firmware which neither Ledger nor Trezor can provide.

Bitfi Knox

Unlike other hardware wallets, the Bitfi Knox never stores private keys on the hardware, which means that hackers have are unable to get to it. Instead, the Bitfi generates private keys on the fly. In a way that doesn't leave them exposed to any connected devices. Nevertheless, the Bitfi Knox is larger than most other wallets and has some issues with usability and with its security features leading to a difficult user experience.

CoolWallet S

The CoolWallet S is another hardware wallet that was designed to fit in your personal wallet alongside your credit cards. The device features support for most major cryptocurrencies and is one of the few waterproof hardware wallets available on the market. The CoolWallet S hardware wallet also comes with Bluetooth connectivity, letting you to manage your funds.

SafePal S1

SafePal S1 is backed by Binance. This device unfortunately is a completely self-contained device that lacks USB and Bluetooth connection methods. It is relatively cheap but it has a built-in camera and six physical buttons which

are all you need to store and access thousands of cryptocurrencies by scanning QR codes on it's associated mobile application.

COLDCARD

COLDCARD is made by the company called Coinkite. COLDCARD has multi-sig feature and it's another open-source wallet which looks like a mini-calculator. The device only supports Bitcoin, which uses a MicroSD backup and provides multiple solutions such as decoy wallets and lockout timers. Coinkite indeed one of the oldest Bitcoin companies on the cryptocurrency market, therefore they are ensuring that this wallet is regarded as one of more secure options to store your bitcoins.

OPOLO Cosmos

Next on my list is the OPOLO wallet. The OPOLO wallet has a 3.2 inch touch screen and works with its own desktop application. The device is both multi-sig and open source and works with over 100 coins and more than 100,000 tokens. It's wallet app has two built in coin swap options, which allows users to swap any coin or token within the application. The OPOLO hardware wallet support a 127 character long password and passphrases and comes with a built in password manager to manage all your passwords.

Cobo Vault

When it comes to the Cobo Vault wallet, it is one of the most secured multi-sig open-source wallets for bitcoins. The wallet works with both its own application and 3rd party applications too, supporting unlimited coin storage for various cryptocurrencies and tokens. The Cobo Vault hardware wallet has a QR code air-gapped feature too for maximum security. Particularly, the Cobo Vault wallet is also waterproof and has a fingerprint sensor.

SecuX W20 & V20

The SexuX Hardware Wallet utilises both web and mobile application and is powered by a 500mAh lithium battery for up to 5 hours of usage. No computer hook-up required. The SexuX Hardware Wallet is not open-source, but supports a wide range of cryptocurrencies and tokens. The device has 2.8 inches large Touch Screen which make the device easy to use while it can

hold over 300 accounts.

Please note that while I am aware of these hardware wallets and seen some of them in action, I personally never used them therefore. So if you are interested in purchasing any of them, you have to do further research. My personal recommendations are the Ledger Nano or the Trezor hardware wallet simply because I have them for years and they never failed me. Yet, I wanted you to be aware that there are more and more Hardware wallet manufacturers on the market competing with each other. Some manufacturer intention is to make hardware wallets smaller while others to create larger wallets with touchscreen. Some wants a better security by eliminating software application support, while other happy to provide continuous software and firmware upgrades to fix bugs and make the device more users friendly. There also wallets that has limited cryptocurrency support with fast functionality, while other wallets has unlimited crypto asset support yet legging in speed of response.

Chapter 26 How many wallets should you have

Well, to address this question and I have decided that first I will count how many wallets I have myself. In terms of hardware wallets I have two Ledger Nano S and one Trezor. Regards to online and mobile wallets I have Blockchain.info, Coinbase, Kraken, Binance, Bitfinex, CEX.IO, JAXX and Exodus. I don't have any paper wallet and I am not planning to have one in the future either. In summary I have 11 wallets but technically each device and hot wallet applications contain multiple wallets, so if I calculate all wallets I ever created for a purpose of transaction, I have over 40 wallets really. If you are a beginner to crypto I would advise you to get first blockchain.info as a hot wallet and a Ledger Nano S as a hardware wallet. Blockchain.info is an excellent hot wallet and you can also start buying bitcoins right away. I would advise you not to buy too much at first until you get a Ledger Nano or a Trezor or any hardware wallet really. Whichever hardware wallet is your preference, it's up to you but you must have a hardware wallet where you can safely store your bitcoins or other cryptocurrencies. When I was new to cryptocurrencies I wanted all in and wanted to have all sort of cryptocurrencies such as Bitcoin, XRP, Ethereum and some really useless tokens too and it has taken some for me to learn that some of these tokens are completely worthless. There are only very few honest projects out there that worth proper attention. Therefore if you are new to cryptocurrencies I would advise you to learn about one at the time. The first cryptocurrency that you should be aware of is Bitcoin. Bitcoin was the first cryptocurrency and everything else is really just a copy. Maybe not all of them, but most of them. And if you think that Bitcoin that is too expensive to buy, well just so you know; you don't have to buy a full Bitcoin. Instead, you can buy for 100 dollars' worth of bitcoins. It's not a lot, but for example my first 100 dollars' worth of Bitcoin I bought is now worth over 700 dollars. My final recommendation if you are a beginner is to get a blockchain.info wallet which is free and then get a hardware wallet. You should also review some of the previous chapter when I discussed how to decide which wallets suits you best. There are few questions you should ask yourself and find out exactly what purposes would you use a wallet. What you are planning in the future. For example if you need a wallet for business purposes, donation purposes, receiving payments, sending payments, investing or trading,

trading with one currency or multiple currencies? But having more wallets is not a problem and you can create as many hot wallets as you wish. The problem with too many wallets is that you need to store all the private keys and passwords somewhere safe. Having a password manager can be helpful, but if you would write both your private keys and passwords on a piece of paper, perhaps having multiple copies of in a safe place would be a good solution.

Chapter 27 Wallet diversification: Scenario 1

Let's imagine that you don't have a hardware wallet yet but you want to buy 1000 dollars' worth of bitcoins. You have ordered your hardware wallet, but you still have to wait few weeks for delivery. Still, you really want to buy bitcoins now because you just can't wait any longer. What should you do? Well, the reason I come up with this example is because I have been there before. Therefore my recommendation is that you try to split across your funds between wallets. For example you buy 500 dollars' worth of bitcoins on blockchain.info, but you transfer 250 dollars' worth to your Exodius wallet and keep the other 250 dollars' worth of bitcoins on the blockchain.info wallet. Next, you go to Coinbase and buy another 500 dollars' worth of bitcoins and transfer 250 dollars' worth of bitcoins to your JAXX wallet. I know that most of the platforms allow you to have multiple wallets but if one of the exchanges or wallet companies get hacked and your investment get stolen by hackers, you would still have 3 more wallets safe. If a hacker would be able to hack one exchange or one Wallet Company, they would try to empty that first. The other wallets would be still secured hopefully. This diversification plan is better than not have one at all and keep on worrying. Once you have your hardware wallet you should transfer all your investments there and keep them safe, unless you are a trader and need your crypto to be moved every day.

Chapter 28 Wallet diversification: Scenario 2

Let’s imagine that you are heavily into Bitcoin and you have more than 1 bitcoins. Let’s say that you already have 2 bitcoins. First of all if you do have at least 1 bitcoin I would like to congratulate you! You are a very rich person. Maybe not yet, but consider this. There will be only 21 million bitcoins ever created while the Earth population is 7.8 billion people. Clearly most people will never have 1 bitcoin and for that reason I suggest if you do have 1 or more bitcoins, you should not tell anyone how much bitcoins you have. Back to our scenario where you have two bitcoins, would you keep them on a hardware wallet? I hope you would. But would you keep them both 2 bitcoins on one hardware wallet? I hope you wouldn’t. Why? Well, the answer is this. Diversification. Please don’t get me wrong. You do whatever you want with your investment. But I will suggest the following. Instead of having 2 bitcoins on the same hardware wallet, have them in 2 hardware wallets. In fact you should have them in multiple Vendor hardware wallets. For example have 1 bitcoin on a Ledger Nano and another bitcoin on your Trezor. Or even better is to have 2 Ledger Nano (1 Nano S and 1 Nano X) and each should hold 0.5 bitcoins. Then you should also get a 1 Trezor to hold another 0.5 bitcoins and have a KeepKey to hold another 0.5 bitcoins. This is to minimize risk as much as possibly can. In case a hacker would ever figure out how to break into Trezor, you wouldn’t lose all your investment because you would still 2 other vendor specific wallets. You might choose to have 6 wallets even you have only 1000 dollars’ worth of cryptocurrencies, it’s completely up to you but I wanted to provide a few diversification plan that you can think of. Moreover, there are few more hardware wallets on the market but I have tried to focus on the ones I know of and being used for years. Ledger, Trezor and KeepKey are the best, safest and most recommended hardware wallets as of end of 2020.

Chapter 29 How to Buy and Transfer bitcoins on Hot and Cold Wallets

In this chapter, I will explain how to transfer bitcoins from a hot wallet to a cold wallet. First of all, once you have a blockchain wallet you might want to buy some bitcoins first. You can buy from any other platform then blockchain.info, so completely up to you but I will explain how you can do it on the blockchian.info site. Once you have a blockchain wallet you can click on “Buy & Sell Bitcoin” and then choose the currency you wish to pay for then enter the amount, for example $300 dollars. Next, you will see that the platform will calculate how much bitcoins you will purchase according to the current market price. Then click on “buy bitcoin”. This will take you to the next page to confirm the transaction. That’s it. You should have now bitcoins, but to send it off to your hardware wallet, you can just simple go and click on “SEND”. This page will ask you to choose the currency you want to send, which in this case is bitcoin, and then you should put in the destination address of your hardware wallet you are transferring the bitcoins to. But if you don’t type in how much bitcoins you want to send off from this wallet, blockchain.info will choose all your bitcoins you have by default. Once you have typed in how much bitcoins you want to send to your hardware wallet, you will also see some transaction fee listed which is normally less than 0.1%. Transaction fees on the Bitcoin network used to be free, but still even in 2020 they are pretty cheap. Before you hit continue you have to type the destination address which is your hardware wallet’s public address. I already explained before how you can locate public address once you have setup your hardware wallet so I won’t get into that now, but you can either paste it in or just simply scan the address. I personally just plug in my hardware wallet, then click on “receive” and then copy the bitcoin address which is the public address, then go back to blockchain.info and paste it in there as a destination address. Next just click on “continue”. Next, you will have another confirmation page where you can double-check your hardware wallet address. The public addresses are very long, so the general best practice to double-check the first and last 3 digits of the address.

Next, if you look at your hardware wallet, you should see that you have received your bitcoins. In case it shows as unconfirmed, don’t worry because normally takes about 10 minutes for each block to be validated on the Bitcoin Blockchain. It might take less than 10 minutes but I have seen it before that

my transaction wasn’t validated for 35 minutes. This mean that the transaction is only got validated 2 or 3 blocks later than the current block. If you want to send bitcoins from the hardware wallet you can just click on send. Then go back to blockchain.info and click on receive and you can just copy and paste that address in a similar fashion as just explained when transferring from a hot wallet to a cold wallet. Put the amount in the required field and just click on “send”. As you see the process of bitcoin transaction is very simple once you get a hang of it.

Chapter 30 Why you must own your private keys

In this chapter, I will talk about why you must own your private keys. First of all, by now you know that most of the hot wallets are easy to set up. You can access them for free and some of them have an ability to buy bitcoins or many different kinds of cryptocurrencies right away. Hot wallets are very convenient, especially the mobile wallets. They are not as secured as the hardware wallets. In the other hand cold wallets or hardware wallets are not free. You also have to wait for them to be received on post. And then you also have to set them up. Unless you know a physical location where you can buy them, still it will take some time to set them up. You have to write down your seed recovery, and then have to confirm those and so on. Hardware wallets are not very convenient but they come with good security. The advantages of the hot wallets are that you can buy coins instantly. For example if a coin price goes down, you can buy very quickly in seconds. Or if you already have some coins kept at your online wallet and the price rises, you can sell them very quickly. The disadvantages are that you leave yourself vulnerable to hacks, especially because all your private keys are online. Also most of the online wallets are only providing wallet access to specific wallets. For example blockchain.info only has Bitcoin, Bitcoin cash and Ethereum wallet. Or Coinbase where there are only Bitcoin, Bitcoin cash, Ethereum and Litecoin wallets exist. So, having a multicurrency wallet like JAXX or Exodus, you are able to hold multiple coins like 10 or even 100s of coins and you can exchange between them which is extremely convenient. Another example why a multicurrency wallet is great is for example if you want to buy some Dash, you have to download the dash wallet. Or if you want to have Zcash, you have to download Zcash wallet. But having a multicurrency wallet, it’s really helpful as you have all the wallets in one place. However the security is not the best and these wallets often get hacked. I understand that cryptocurrency traders need anytime access to their coins and fast. Traders are taking a risk but they are aware of the potential risk or at least they should be aware. So, when it comes to hardware wallets like Ledger Nano, Trezor or Keepkey, the private keys are generated offline on the device and they always going to be there. Thus any online attacker would not be able to have access to your funds. There is just no way. Another advantage to hardware wallets is that if someone would have physical access to it, they

wouldn’t be able to use it without your private keys which should be keeping far away from your device as I pointed out earlier. Likewise if you would lose your hardware wallet you can just buy a new one. Having your seed recovery sheet you can just regenerate your private keys once again. The disadvantages of the hardware wallets is that they are not as convenient as most hot wallets. You have to plug them into your computer with the small USB connector and you cannot just exchange between coins in seconds. Instead, it any exchange or transfer will take minutes. If you are serious about Bitcoin or other cryptocurrencies you must have a hardware wallet. I have a lazy friend who has 3 bitcoins and still don’t have a hardware wallet. He might never get hacked, but why would you take such a big risk if you can just buy a hardware wallet, learn how to use it and sleep better at night. The way I look at wallets is that any hot wallet is only for buying and hardware wallet is for storing currencies. So even if you are a trader, when you make some profit you should keep that profit secured in a safe place. The only solution for that is having a hardware wallet. I hope that you see where I am going with all this simply because security is very important. I am sure that you wouldn’t leave your money out to the open for thief to access it easily. I also understand that some people have no money for hardware wallet or feel like the hardware wallets are too expensive or just lazy to take their time to learn about it. But please understand that there is a reason why these devices are expensive. Think about this example. Imagine that you have 5000 dollars’ worth of cryptocurrencies but the cheapest hardware wallet cost 300 dollars. Would you not buy a hardware wallet so have a piece of mind? I hope you would as I do. Once again when you have a bitcoins you are the bank and that comes with responsibilities.

Chapter 31 Hot Wallet Hacks

First and foremost, I will talk about the famous MTgox hack. MTgox was one of the largest Bitcoin exchanges that were based in Japan. They have started trading bitcoins back in 2010 and by 2014 they have been handling 80% of all bitcoin transactions internationally. Most people have heard that MTgox has suspended all bitcoin trading in 2014 and filed bankruptcy. But the first hack was actually in 2011. In 19th of June 2011 there was a security breach when a hacker took over the MTgox site, and begin to transfer bitcoins from costumers hot wallets to himself, driving the Bitcoin price down from 17 dollars to 1 cent. This hack only taken about 5 to 10 minutes, and after 10 minutes the Bitcoin price has become stable again at 14 dollars. But at the time about 600,000 bitcoins were stolen from customers. Some people called this event a flash crash or Bitcoin price crash, but it was a security breach at the time. MTgox have been compensating their customers from their profit but by 2014 they had to suspend all trading as over 300 customers have been complaining that they are missing some of their bitcoins from their MTgox wallet. So MTgox has suspended all trade in order to take better look at what is actually happening, and realized that they are missing more than 850,000 bitcoins. In 2015 after more than 1 year of investigation they have realized that hackers have been moving bitcoins from customer's wallets from the online exchange since 2011. Ever since they have only had recovered 200,000 bitcoins but the rest of them are all stolen. When MTgox were at the court hearing they said that they have lost around 750,000 bitcoins from their customer's wallets and 100,000 bitcoins which they have owned totalling 850,000 bitcoins. In 2011 there were no hardware wallets yet so this very unfortunate. But there are many similar Exchange hacks since we have hardware wallets on the market were customers lost their investments, which I will discuss shortly but this is just another reason why you should not keep your bitcoins on an exchange wallet or hot wallet any longer then it's necessary. Moving on, the next company on my list is called Bitfinex. Bitfinex is the one of the largest Bitcoin exchange since 2014 based in Hong Kong, trading more than 10% of all bitcoins amongst all other trading platforms. Nevertheless Bitfinex have been hacked in 2015 and the hackers have stolen 1400 bitcoins. According to Bitfinex they only lost about 0.05% of their Bitcoin holdings, so they have carried on business as usual. However

later on in 2016 August they have announced that they had a cyber-attack and 120,000 bitcoins have been stolen from customers' accounts. Bitfinex was able to pay back every customer their missing investments, but it took them a year and a half and they paid back everyone in dollars not bitcoins. Moreover, Bitfinex only paid back the amount what customers were paying for the Bitcoin price at the time they bought them not how much they were worth at the time of the hack. At the time of the hack, the stolen bitcoins were worth about $70 million dollars but Bitfinex have been able to compensate their customers and the business is back as usual ever since.

Next, on my list is another company called Bitstamp. Bitstamp was founded in 2013 which is also a Bitcoin trading company based in Luxemburg. Bitstamp also trading with other currencies among Bitcoin and became very popular but in 2014 they have been receiving continuous denial of service attacks and the hackers have demanded the Bitstamp to pay 75 bitcoins in order to stop the attack. They have paid the ransom and they have enhanced their security, still nearly a year later Bitstamp have been hacked again and hackers have stolen 19,000 bitcoins from their platform.

Moving on, in 2016 May a company called GateCoin was hacked and 250 bitcoins and 185,000 Ethereum was stolen. GateCoin was one of the first regulated cryptocurrency exchanges at the time and its fame made it a prime target for hackers. They have gain access to user wallets and stole cryptocurrencies valued at 2 million dollars. After that, GateCoin has never recovered. Next, in 2017 4,736 bitcoins were stolen from the company called NiceHash. NiceHash is a cryptocurrency mining marketplace that allows miners to rent out their hash rate to other users. Their payment system was compromised, causing users Bitcoin wallets to be stolen. The exact amount stolen was never confirmed by NiceHash, however it is believed to be 4,736 worth of bitcoins, worth about $62 million at the time has been stolen. In the end NiceHash returned 60% of the stolen funds to users but still over $20 million was never recovered. Next, in 2017 July, $7 Million Worth of bitcoins and ethereum were stolen from a company called Bithumb. At the time of the hack, Bithumb was the third largest cryptocurrency exchange by volume worldwide. Still, a hacker managed to gain access to an employee's personal computer and stole the details of over 30,000 Bithumb users. Shortly after that, users started noticing their accounts being drained of crypto. Moving on, in 2018 April, 428 bitcoins were stolen from a company called

CoinSecure. CoinSecure is an Indian cryptocurrency exchange which lost Bitcoin valuing $3.2 million at the time of the hack. Nevertheless, it seems like this one was an inside job. The owners of the company believe their former CSO aka Chief Security Officer stole all those cryptos who was later arrested. Moving on, in 2019 June, Bithumb was hacked again and this time the hackers have stolen $31 Million Worth of XRP. This hack seems to be orchestrated by a group of North Korean hackers known as the "Lazarus Group", who have been in charge for a number of cryptocurrency hacks over the last few years. Bithumb promised to pay back any stolen funds. In 2019 May there were 2,578 Ethereum stolen from a company called Taylor. Taylor is a cryptocurrency trading application that raised a successful ICO aka Initial Coin Offering to get funding. Awkwardly, not long after, hackers gained access to a company device and took control of a password file. The hackers stole all the Ethereum raised at the ICO, valued at 1.5 million dollars. Next, in 2019 September 5,966 bitcoins were stolen from the company called Zaif. This is yet another case where it's unclear how hackers stole all these bitcoins. Zaif did file a criminal case with their local authorities, which makes it sound like they have an idea as to who did it. Still this Japanese exchange has lost 60 million dollars' worth of bitcoins. Next in 2019 October 913 BTC were stolen from the company called MapleChange. Many believe this hack was part of an exit scam. MapleChange was a small, Canadian cryptocurrency exchange that began to see a spike in exchange activity starting in October. Later on, the exchange announced that it had been hacked and all funds had been withdrawn by hackers. At the time it was valued at $5.7 million. Next, MapleChange announced it was closing its doors for good. People still suspicious about the immediate removal of the website, social media accounts and Telegram channels and many believe that there was no hack despite the company insisting they were just taking a short break to decide how to proceed instead of deciding to pay users back the money they claim to be hacked. People still unsure if it was a hack or just another exit scam. Next in 2019 January at least 19,000 ethereum was stolen from a company called Cryptopia. First reports were Cryptopia users having difficulty accessing their accounts, then eventually users realized their accounts have been drained. The company first thought it was a technical issue, yet later clarified that it was a security breach. The exact amount stolen in the hack is still unknown but it is estimated that at least 19,000 ethereum was stolen. Moving on, in 2019 March there are 3 Million EOS and 20

Million XRP were stolen from a company called Bithumb. Bithumb is a South Korean cryptocurrency exchange seems as it was the victim of an insider job. The hack began with a suspicious withdrawal and the company instantly suspended all withdrawals on their platform, however it was too late. Whoever piloted the hack is still unknown. Since the hack there is no evidence of outsider and many suspect that it was an insider within Bithumb who stole the cryptocurrencies. Moving on in 2019 March there are $7 Million Worth of bitcoins were stolen from a company called DragonEx. DragonEx is a Singapore-based crypto exchange were hackers stolen $7 million worth of cryptocurrency. The North Korean hacking group called Lazarus was accountable. The Lazarus group created a legitimate looking fake website and convinced DragonEx employees to download malware onto their computers using LinkedIn messages. DragonEx has taken full responsibility for the hack and started issuing refunds to those who lost their money. Moving on in 2019 May, 7,000 bitcoins were stolen from a company called Binance. This time the hackers were using a phishing scam and malware to hack into Binance platform and stolen $40 million worth of bitcoins. After the hack, Binance promised to increase its security, but it seems that customer data may have been stolen too. In August 2019, someone online began sharing customer verification information from Binance on another well-known trading platform called Telegram. It seems that this data was also taken during the hack and over 60,000 users may be affected. In 2019 July a company called Bitpoint was hacked where hackers manage to steel 1,200 bitcoins, 11,000 ethereum, 1,800 bitcoin cash, 5,100 litecoins and more than 28 million XRP. After seeing an error in its outgoing funds transfer system, this Japanese platform instantly suspended its services. Nevertheless, it was too late. Hackers manage to steal over $30 million worth of various cryptocurrency. Bitpoint was able to recover $2.25 million of the stolen crypto from overseas exchanges and said that they will compensate their users, while not released a time frame as to when that will occur. This year in 2020 February a company called Altsbit has been hacked were hackers stolen 6,930 bitcoins, 23,120 ethereum and various other cryptocurrencies. Altsbit is an Italian based cryptocurrency exchange which only been trading for a few months before it was hacked. Firstly, the exchange announced the hack stating that almost all funds had been taken but later on realized that only about half of their cryptocurrencies were gone. Altsbit also announced that it only has enough funds to issue partial refunds

and they will be closing their doors in 2020 May. It seems that the Hacking group called “Lulzsec” was behind this hack, as they claimed that they are responsible, however it is still unclear how they managed to deploy this hack. Roughly $70,000 worth of cryptocurrency was stolen. The reality is that I could go on and on about these online exchange hacks but I just wanted you to know that until you don’t have your cryptocurrency on your own cold wallet, they are not safe. Moreover, do not forget rule number one, which is this: If you don’t own your private keys, you don’t own bitcoins. To have your own private keys, you must have your own physical hardware wallet.

Chapter 32 How to avoid Hardware wallet scams

There are many scams to watch out for especially when you see a huge price fluctuation of bitcoin and other cryptocurrencies. I can't list them all as here because scammers are always evolving using new and better techniques day by day. But there are a few scams I can list you should watch out for that are out there. I see few people posting on the internet asking about suspicious text messages they receiving that sounds similar to this:

"Ledger alert!

Dear Customer, Our software has a critical bug with the risk of losing assets. Please visit usaledger.com and update it ASAP!"

So if you receive a text message like that please do not click on the link. Do not click on any links even if it sounds legit. In fact do not click on links within email from suspicious senders either. If you do, your system could easily get hacked. Ledger users are constantly targeted by phishing attacks on social media, search engines, text messages and via email. Hackers are able to perfectly copy Ledger's genuine website, applications or content to pull users into entering their 24-word recovery phrases. Therefore you have to be very careful. In case you're asked to provide your recovery phrase or asked that you should send cryptocurrencies to anyone, remember that it's a malicious attack. In terms of best security practices just remember the following. Anyone who has access to your 24 word recovery phrase also can have access to your cryptocurrencies. Also, you should never enter your 24-word recovery phrase anywhere else other than on your hardware wallet. Also remember that Ledger or Trezor or any hardware wallet manufacturer will never ask you for your 24 word recovery phrase. Lastly, if you receive any messages or emails related to any update or anything that makes you want to click on links they provide, instead of clicking on their links, use the official contact form the hardware wallet's website by visiting the website by yourself. There are other malicious attacks too such as fake Chrome applications. Fake Chrome applications can install keylogger to your browser using automated systems. The keylogger software alone would not steal your cryptocurrencies, but if it's automated correctly, it can send signals back to other software when you are entering a destination address to send cryptocurrencies. At this time a fake Chrome application can deploy a MITM

or Man in the middle attack and paste the hackers public address, making you sending cryptocurrencies to the attacker. There are also fake recovery applications as well fake competitions where they ask you to provide your 24 word recovery phrase so you have a chance to win 10 bitcoins. This is also a scam. Basically scammers try to convince victims that they need the 24 word recovery phrase to know where they have to send the bitcoins. But this is a scam because if someone wants to send you bitcoins, you only have to provide your public address and not the 24 word recovery phrase.

Another scam is where you see fake YouTube and Facebook live streams from malicious actors. This time they often create urgency by saying that the first 100 people who participate on their website which is a phishing website; they will receive 10,000 dollars' worth of bitcoins or ethereum. This makes victims falling into the trap. They click on the link of the phishing website which is an excellent Ledger or Trezor looking replica where you will find a few questions that you have to answer quickly. They start off with some basics, such as your name, what kind of wallet you have, your pin number to your hardware wallet, what kind of Browser you are using, your 24 word recovery phrase. While the victim would begin to think that is something wrong, they would be distracted because the phishing website would have a clock counting backwards to create real urgency. Therefore many victims quickly find their Seed Recovery sheet and provide their 24 word recovery phrase. Unfortunately, these attacks are getting better and better every day, therefore you always have to be cautious. Additionally, I strongly encourage you that if you are affected with any of the above mentioned scams or phishing attacks; you must file a police report in your jurisdiction as soon as possible. As a last reminder, you must maintain your web browser and keep it updated with the latest upgrades. You should always carefully review suspicious emails and text messages. You should always be suspicious of links and be watchful when asked to install any software. And you should never type your recovery words into anything other than your hardware wallet.

Chapter 33 Best Practices to Guard against MITM attacks

Hardware wallets are the most secured devices but unfortunately there is never enough security, especially if there are humans involved. If someone has access to your seed recovery that person can use those to recover your wallet. But bad guys can also use other techniques to steal your money by implementing a man in the middle attack. The most common way that people losing their bitcoins is that they are typing the wrong address as a destination and sending their funds to the wrong address. There is a way to trace the address but it takes a long time and if the recipient sees that he has received large sums he might withdraw those quickly and you will never see those bitcoins again. I have seen people posting all over the internet that suddenly they woke up and had 60 bitcoins on their wallet and now they don't know what to do. Also heard arguments where people said that they deserve to lose their money if they don't know how to make a simply bitcoin transfer. Well, sending bitcoins to the wrong address can be a mistake but hackers also found their way around it by remote accessing computers and pasting their own address to receive bitcoins. Hackers can infect computers with a special malware and once the node is compromised the attacker can change the code used to generate an address and paste their own address. This is also known as MITM or Man in the Middle attack. What you can do to guard against the MITM attack is to use your hardware wallet on a laptop or computer that is malware free. Use a device that you only connect to the internet for payment purposes and nothing more. Besides, you should double-check the address that you are pasting in making sure that you are using the intended address and not a different address. I know that checking every letter can take a long time but double-checking the first and last 3 digits of the address are good enough practices. Also, when you connect your hardware to your computer, make sure that you disconnect it once not using it anymore. It will disconnect itself after 5 minutes but you should manually disconnect it. In case you catch someone in the act you must disconnect the device immediately! If that ever happens to you then your computer is definitely compromised and you must do something about it right away! Hardware wallets are safe but when you interfere with the internet and your computer is compromised that's a different issue. Therefore you should make sure that you have a good antivirus installed and updated accordingly so you have no malware infection

on your device.

BOOK 5

CRYPTOCURRENCY INVESTING

17

PRIVACY BASED COINS YOU SHOULD KNOW ABOUT

BORIS WEISER

Chapter 1 Defining Anonymity

The word anonymity is coming from a Greek word: Anonymia, which simply means without name or nameless. The word: Anonymous is in use to describe situations where the acting person's name is unknown. The idea here is that a person non-identifiable, unreachable or untraceable. For example anonymity is enforced by low when people voting in free elections. Many other situations like talking to strangers or buying a certain product or service in a shop, anonymity is traditionally accepted as natural behaviour. For example if you stop someone on the street and ask the time; "excuse me, do you know what's the time?" You don't have to introduce yourself. Same thing applies when you walk into a supermarket like Tesco and buy some bread and milk and make payments by yourself using cash; you are basically shopping anonymously. If you make a payment using your bank card, the payment would be traceable and that would NOT BE an anonymous shopping experience. There are many other situations in which a person might choose to withhold their identity. For example an act of charity can be performed anonymously when the benefactors don't want to be acknowledged. Another common example is if you witness a crime; you can choose to be an anonymous witness. In the other hand, crime can be carried out anonymously too. As you see, being anonymous can be used for good as well as for bad intentions. Anonymity can be chosen if you are a writer or editor but there are also anonymous advisors in business and politics and other areas; but our focus in this book will be on internet anonymity. There are various software exists to help anonymity and probably you heard one of the most famous one called: Tor or also known as the Tor Browser, The Tor Project or sometimes referred to as The Onion Router. The Tor Project it's a free software that provides anonymous communications and web browsing on the internet but there are many other projects similar to Tor; revolving around the concepts of anonymity created by the Cypherpunks which I have talked about in more detail in my other book called Bitcoin for beginners. By definition, Anonymity on the internet applies to any interaction a user has on the internet that protects his or her identity from being shared with another user or with a third party. There are different anonymity levels exist and examples of anonymity can be seen all over the internet. Some of the most common examples of anonymity on the internet include: Q&A sites or questions and

answers where users use anonymity which allows people to ask questions of known users to obtain responses. Similarly, there are Anonymous blogging and posting where users are able to blog and comment anonymously. For example sites like Twitter or 4Chen you can post links anonymously. The most common anonymous sites are related to flirting and networking where users are able to flirt with others while remaining anonymous. Lastly, I will mention the one that is also one of the most common anonymity on the internet and the most relevant to this book's topic which is secure billing. For example when a user purchases something with PayPal on Ebay; the user does not reveal his or her personal information to the distributor. While this is true, PayPal can see all your transactions and also can limit or disapprove certain transactions. PayPal is a trusted third party and the point of cryptocurrencies in the first place is to avoid trusted third parties. In the next chapter I will talk about who would use privacy based coins.

Chapter 2 Why Privacy coins needed

One of the major topics are all over the headlines in the cryptocurrency world is nothing other than privacy. And one of the main reasons why Bitcoin got adopted in the first place is indeed privacy. Cryptocurrencies wouldn't be where they are today without that little sense of anonymity of privacy. However, the reality is that Bitcoin and it's leading competitors are not providing full privacy, and this is because every single transaction is visible on the blockchain. This issue have been causing fear for a while, and lots of people began to search other alternatives then Bitcoin. When you think back in time the way we used to transact, cash was one of the best solutions for privacy. There are other ways to negotiate amongst us using other alternatives such as Checks, Wire transfers, Credit Cards, Swift or other trusted third parties such as PayPal or Payoneer; still none of these mechanisms are providing anonymity. I am not saying that these solutions didn't help us, in fact they still exist and probably won't go away as smoothly as some might want to. Nevertheless, these types of solutions are decreasing our privacy. For example you might don't have any problem sharing with the world where you spend your money, yet a large percentage of people do prefer privacy. Either way, cash or paper money is one the best model to look at, especially the way it works in real life. Money exchange in real life is what really should be enhanced for the internet. Here is what I mean; if I give you a 10 dollar note, then you give it to your friend, there is no direct link where that money came from in the first place. For example, the bank can tell how much money I have on my bank account; but the bank can not know precisely how much cash I have in my pocket. Paper money has serial numbers and somewhat can be traced, but the amount of paper money I have in my pocket, only can be revealed by me. Still, cash is regulated by the government, and it can be easily counterfeited; therefore cryptocurrencies can become an excellent choice to replace paper money. Privacy is not all about criminals as there are ordinary people who also prefer privacy, instead of publicity. For example, most people prefer not to advertise their spending habits. Personally, I don't want the world know what I just bought from a certain website last week. Back to Bitcoin, it is somewhat anonymous, but if you give me your wallet address for the soul purpose of making a payment to you, it will be validated on the blockchain. The problem is that blockchain

not only recording the transactions I have initiated to you, but all purchases that you and I have ever made. We will see each other's funds which we have control over with those wallet addresses that is yours and mine. The following link shows all live Bitcoin transactions taking place:

https://www.blockchain.com/btc/unconfirmed-transactions

Here, you can see who sent to whom and how much bitcoins. You can also see all old transactions as well for each wallet address while you can also see how much bitcoins were ever sent and received on each wallet, or how much each wallet holds currently.

If I choose to pay someone with bitcoins, the person I am paying can see all my transactions and my wallet can become a target. Business relationships are also something that I should mention here. In the future we can have a decentralized trading platform where we could keep all our funds. When it comes to online shopping there are less than 10% of people who care about their privacy. But when paying with cryptocurrencies, we are moving to a different level. The 90% of the people who don't care much about online privacy, they say that because it's all about online shopping. But using fiat currencies such as paper money to pay someone online, the person you are paying cannot reveal how much money you have on your account. Neither you can see how much money he has on his account or how much money he ever received or spent previously. Still, all bitcoin transactions are on the Bitcoin blockchain. There are already few privacy based coins exist which are now solving these issues. Some of these privacy coins are running on a specific blockchain but back to the question; who would use privacy coins? As I said it's only about 10% of the population who interested in privacy payments and if you think it's not a lot, then let's look at the figures instead. The current World population is 7.6 billion and if you look at the 10% of that figure you can end up around 760,000 people who really keen in this subject. Those 90% who would say otherwise might not necessarily true don't care about privacy, especially if you consider the fact that people who says they have nothing to hide, most probably want to hide something. Those people might have nothing to hide right now, but could easily experience a moment in their lifetime when they wish to pay someone anonymously. They might want to support someone by donating few bucks or perhaps paying a charity. There are several reasons really why one might need to make an anonymous payment at some point but privacy based coins are optional. When it comes

to cash payments with paper money, you most probably have to be present at the payment for a product, but if you want to buy something online using traditional banking system, your payment will be still traceable. Your payment using traditional banking system could also be denied if the bank wishes to do so. It depends on what you are trying to buy and I am certainly not advising to buy anything illegal online. Online shopping should be borderless. Similarly to what cryptocurrencies represent. But some products are legal in some countries while the very same products could be illegal in another. If your bank decides that you are involved in a possible illegal activity not only your payment wouldn't go through but they would probably freeze your account and call the police on you. Banks will not give you options for anonymity. If you want to make a donation for a charity anonymously using traditional banking system you will have a hard time to do so. Privacy based cryptocurrencies are optional and no one forces you to participate. Evan if you will never going to have any interests in privacy based coins and anonymous payments, you might find someone who you can help by explaining that the solution for their issue already exist. Shortly I will reveal the most well-known privacy coins and you can decide which one you prefer best.

Chapter 3 Cryptocurreny Basics

In this Chapter I am going to talk about what is a cryptocurrency. A cryptocurrency is a digital currency where cryptographic proofs used for validating transactions instead of trusted third parties. In the other hand, many people believe for example that ripple is a cryptocurrency. Ripple is a very valuable protocol which can be utilized to send a centralized currency. The developers of the Ripple project have assigned a native token to Ripple called XRP. Still, the XRP transfer validation process is happening by humans and not by cryptographic proofs. Therefore Ripple is a perfect example when the word cryptocurrency should not be used because while there is a transaction, they don't use cryptographic proof, neither when XRP token is created. Some people might get disappointed on this statement but that's just the reality of it. There are hundreds of similar so called cryptocurrencies on the market for a purchase, but they really have nothing to do with cryptography. Therefore they should be called a centralized database and nothing more. Moving on to the most important subject that allows cryptocurrencies to exist in the first place is called Blockchain. Blockchain is a decentralized ledger system and if you know how banks work it's similar to that system. Banks have ledgers, ledgers have accounts and accounts have balances. However the key difference between the banks and the blockchain is that banks have centralized ledgers while the blockchain is decentralized. Additionally, in order to make a digital payment with your bank card, it must go through banks where humans would authorise the payments. While the blockchain is decentralized and instead of humans, computers validate transactions using cryptographic proofs. There are lot more into it and I have explained what the blockchain is and how it works in more detail in my other book called Bitcoin for Beginners. The key is really to cryptocurrencies are decentralization and cryptographic proofs. In terms of Altcoins, stands for Alternative Coins or Alternative cryptocurrencies, you need to remember that Bitcoin was the first ever cryptocurrency therefore every other cryptocurrency is an Altcoin. For example Bitcoin Cash or Dash, Monero, Litecoin, Ethereum, they are all Altcoins or Alternative cryptocurrencies. Still, there are many so called cryptocurrencies out there and they claim and advertise themselves as they are using blockchain technology. In reality they only represent a centralized system, or centralized database, therefore they

should not be called even a cryptocurrency. I will provide some technical analysis on some of the most famous privacy based coins where you might realize that they are not as anonymous neither decentralized as they claim to be. To understand how some of the cryptocurrencies work, it’s good to have some basic understanding of the fundamental terms, as it seem that most people believe all the marketing speeches, instead of questioning the underlying technical or functionality related aspects. You might get surprised that some of the most well known cryptocurrencies in the space just can’t be functioning in the way they describe them especially once you break down to fundamentals. I will explain more on this topic later on when I will introduce some of these cryptocurrencies.

Chapter 4 How Privacy Coins Work

As mentioned earlier, bitcoin transactions are visible on the blockchain but there are no names or bitcoin owners are visible therefore bitcoin (as in the end of 2020) is a semi-anonymous cryptocurrency. Bitcoin wallets are providing specific names publically but they are often can be traced back to individual users through transaction history, service providers or even by IP Addresses. To overcome these issues, so called mixers were introduced. Mixers are in this case a collections of people who came together to share token, mix them up, and then redistribute them. This makes it more difficult for individuals to be linked with specific tokens. Nevertheless, some other currencies are going even farther to protect users anonymity. Some technology features are allowing users to pre-mix their coins during transactions and many privacy based coins are using these kinds of methods. But, they can be still potentially be traced by expert analysers. In the other hand, some other cryptocurrencies using ring signature system in which multiple users share a set of keys. Ring signature system confirms transactions without revealing which of those users were party to the transaction. There are also other privacy based currencies using proof of work algorithm with no transaction history whatsoever. Overall, there are different ways to go about creating anonymity and I wanted to give you a high level overview before I get into more technical details on each of the best anonymous cryptocurrencies.

Chapter 5 ICO Insanity

Let me explain quickly what is an ICO. ICO stands for Initial Coin offering. ICO sounds like an IPO but IPO stands for Initial Public Offerings. IPO-s are regulated while the ICO-s are not regulated or at least not controlled yet. ICO-s are happening when a particular company raises funds to distribute a token to their investors. It is somewhat similar to crowd funding which is also an excellent way to engage with the community and allowing people publically to invest into the company's funds in exchange for distributed shares. Before getting into the history of ICO-s, how they work and why people would come up with new ICO-s, in this book I am covering only the best privacy based cryptocurrencies so I am only covering ICO-s in high level overview. This is so you are aware of the term and its existence related to the cryptocurrency market.

The first ever ICO happened when Ethereum was born. It was the most successful ICO but ever, since ICO-s are popping up all over the place. Literally, there are new ICO-s coming to the market daily, and for that reason it is very difficult to learn about them all. There are some really good ICO-s, truly honest projects but also many of them turns out to be a huge scam. Often the developers only have one intention which is to collect lots of money for their project and then run away it the money. Especially 2017 was the year of the ICO-s and it seemed that 80% of the projects were nothing but scams. By the end of the second quarter of 2017, we have learned that more then 85% of all ICO-s were scams. But by end of 2017 we have realized that 99% of all ICO-s are definitely scams. Take this as a warning and understand that ICO-s exist and while lot's of people became making money, many more people have lost all their money and became very poor. I will cut to the chase right away and advise you to stay away from ICO-s. While it's nice to support someone's project and also great if you get reward from the company, ICO-s are basically raising cash for their own projects. Most times there is an ICO when there is no product on the market yet. So an ICO is considered to be initiated by a centralized entity who can pull the cards anytime and turn around saying anything they want. They might say that the project that they really wanted to create it's not feasible due to technical issues. But of course they tried everything they could. In the meanwhile all the money is gone for the project. It's basically a nicest way to say that:

“Sorry that the project failed, but we can’t give your money back.” I will give you some examples so you can understand what I mean. One of the most well known scams were the one called: Onecoin. Onecoin has been presented as a new ICO but turned out to be a major scam. Unluckily, many folks have lost their life savings due to capitalizing into this fake cryptocurrency investment. Those who endorsed this project have been sent to jail already in India as well in Dubai. The business was formed in Bulgaria with the purpose of anticipating to find gullible individuals around the world and sell them Onecoin and constructing a believe that they’ll all become rich. The issue was that you were only able to buy Onecoin from the distributors; but once you wanted to sell, you were not able to. This scam was achieved by the distributors who wouldn’t repurchase the coins from you. And if you though that you can find an online exchange, or someone who would buy it from you, think again. There was no exchange who would deal with this particular coin therefore it had no value. So, how did people fall for the Onecoin scam? Onecoin was promoted as a next possible Bitcoin and they have created adverts where they advertised Onecoin and Bitcoin in the same sentence or in the same picture. This tagline caught people’s attention and they began to purchase it. But once they realized this project has never made it any further, people wanted to sell it but it was too late.

The next huge crypto Ponzi scheme I will briefly describe is the famous Bitconnect. Bitconnect was running one of the biggest Ponzi scheme in the space which made many people very rich while others have been suffering and loosing all their money they have invested. Bitconnect allowed you to put in a loan and they promised to return your loan within 240 days. But before your investment would be returned back to you, you would get 1% interest on that loan every single day. So, for example if you have given them 1000 dollars, you would get back 10 dollars a day for 240 days which would come to around 2400 dollars / year on your first investment of 1000 dollars. So, you would end up by 2400 dollars profit within 240 days. Of course it’s sounds to good to be true. When Bitconnect has announced that they are about to shut down their lending exchange, everyone was panicking. While bitconnect promised to refund everyone, they did it by paying everyone in bitconnect token which became completely worthless by then. The market capitalization has fallen off from 2.7 billion dollars to 200 million dollars in about a week. Many people lost their lifesavings and some committed suicide. The real problem was that people were greedy. Everyone knew that

this is a scam and probably not going to end well but they were making so much money (on their monitor at least) that they just didn’t care. What you can learn from these ICO scam tokens and Ponzi schemes is that while I will expand on some of the best privacy coins, you have to understand that investing in the cryptocurrency market is very dangerous. Therefore you should not take me as your financial advisor, instead understand that any coin you participate, you will do it for your own risk. Later on I will also explain what you can expect from cryptocurrency regulators too such as SEC, CFTC or FinCen.

Chapter 6 How to avoid being scammed

I have talked about some of the major well known scams in the cryptocurrency space like Onecoin and Bitconnect, but there are thousands of other scams out there. There are so many scammers around the web that is just very difficult to say which ones are legit, especially for those new to this market. Once you have some experience you will know how people with bad intentions are trying to scam people using Ponzi schemes and other methods. But, how do these scammers reach potential victims? They use multiple techniques. The most common ones are that they leverage trustable, known platforms and pushing an aggressive marketing. Basically they would go where the people are. Those might be Facebook, Twitter or YouTube where they begin to video ads, trying to make you believe they will give you a huge profit margin or even make you a millionaire. Often they are using techniques such as creating a fake Facebook account or YouTube channel or counterfeit websites. They do in a convincing way so people would fall for it. Let me give you some tips on how to avoid these scammers. First of all, anytime you hear things like double your money or making a profit every day, there is something dodgy going on. Unfortunately, there are many people losing thousands of dollars because they fall for some of these scammers or thieves and there is not much they can do about it. So let me give you some specifics on how these people operate and what you should look out for

Scam alert No1:

Scammers put pictures of famous people on the website. But on these websites you cannot find information about the CEO or the link of “About Us” does not work or worse, there isn’t one. There are some occasions where the “Contact Us” menu option isn’t working or there isn’t one on the site at all. These should be a big red flag right away.

Scam alert No2:

Unreasonable high return. Anyone who claims that you can double or triple your money it is most probably a scam. In the crypto world no one can tell you exactly what the market will bring us. It is possible to double or even triple your money but if someone guarantees that, it is most probably a scam.

The value of Bitcoin took about two years to less than a cent whiel as of the end of 2020 the price of is hanging around $19K. Nevertheless there is no guarantee for another 2X or 10X by end of 2021 or 2025. For example I personally do believe the price of Bitcoin will reach easily a $100K at some point but neither I nor anyone else can guarantee that for certain.

Scam alert No3:

Unsure the purpose of the company. Sometimes if you go to a website of a token, and can click on the “About Us” menu option (if it works of course) and you find that you are not 100% clear on what the company does exactly, that could mean a possible scam. Some might say that they are trading for you, but then how do they make up for their profit?

So if you can contact the company you should ask them questions such as:

- What is the company does exactly?
- How do they guarantee you investment back?
- How do they ensure security?

If you get a response that is a bit wishy-washy, then probably is a scam. If they don’t even reply to you at all, then again, it is possibly a scam.

Scam alert No4:

The particular coin is not listed on https://coinmarketcap.com/ If you cannot find a coin that you are interested in CoinMarketCap, then most probably you should stop looking into that project. It’s not necessarily a scam but if hear about a new cryptocurrency or token, do not go to their own website and start investing without any research. First you should always check CoinMarketCap. As a side note, even if the coin is listed on CoinMarketCap, it could be still a scam. For example Bitconnect was listed on CoinMarketCap for over a year when suddenly taken off. But if the token aro crypto asset you are looking into is not even listed on CoinMarketCap, then you really should be cautious and do more research before investing.

Scam Alert No5:

The coin is centralized. Once a certain system is centralized, it is controlled by an individual or a company. If it has a central Server, which can be monitored; there is no guaranty that they will not go and alter it or to make any changes without telling anyone else about it. I could go on and on about possible scams, as well how to recognize them, but if you are a newbie, you might find it useful that there is a dedicated website for Bitcoin or other cryptocurrency scammers called: https://behindmlm.com/

This website is a collection of scams and Ponzi schemes where people reply to one another and explaining experiences of different websites. Once again, please be extra vigilant, and research on any trading company before you would invest into it. Double check their website but even if you find it extremely professional but even then you should try to contact them. When you contact the company, you should ask questions that might concern you. Genuine companies should get back to you within 24 hours due to time differences and they would provide you with an answer that you were looking for.

Chapter 7 Pump and dump

Once you get into the world of crypto, you will often hear people saying "*Pump and dump"* . If you hear someone says for a particular coin or token that is just a pump and dump, you should investigate it. If it happens to be true and the particular coin is really just a pump and dump and you already invested to this coin, you should probably get rid of it as soon as you can. Let me elaborate on this topic and explain how pump and dump really works. In case you never heard of the term pump and dump, then don't worry, once I will explain it you will remember it forever. The process is relatively straightforward. Let's start by saying that is an illegal activity. Pump and dump scams comprise two groups of individuals. First, there are the performers who falsely increase the price of a certain coin by promoting or endorsing it. They begin to buy the fake cheap coins or tokens and while they build up a hype using social media platforms and marketing. Once the hype builds up around the fake coin, the trading volume began to increase and the token or coin value goes up. The person or group is also known as both; the pump and dumper. Once the coin hits the wanted price, the performers sell all their coins and people begin to panic. Meaning they all too start to sell and dumping their coins to the market and making the price to drop. In order to notice a coin that's being in the picture for a pump and dump, it's relatively easy. You'll often see buying patterns by the price is falling and rising just considerably each time the performers buy, stacking up on the cheap coins without showing too much attention.

Once they've purchased the coins, the performers going to post on blogs, forums and chat boxes and explain several reasons about the new coin why this is so good of an investment. They'll use several different accounts; but there might be more people involved in this illegal activity to make it more believable. This can be achieved by paying off YouTubers especially those already have large followers. Pump and dumpers will ask YouTubers to make at least one or several video's talking about their coin. These video's generally has to be positive about the tokens and the YouTubers should be endorsing both the token and the company issued it. That's just another illegal activity especially when the YouTubers are not mentioning that they are getting paid to review a particular token. Often these YouTubers are actually innocent as they don't know much about cryptocurrencies nor never

do researches on Fin-Tech companies. Directly or indirectly, YouTubers will continuously talk about the coin until there the hype is big enough and people begin buying those particular coins. Once the audience fall for it and start buying it, the pumping happens again. In the meanwhile, scammers might even go as far as tell you what are the best platforms it to buy the coins to direct followers to the site and get them purchase as much as possible. This process pushes the hype even further and more people begin to buy because they see the coin price rising. Once the coin hits the wanted high point, the performers start selling their coins but not all their coins in the same time. This is the time when you should see that the dumping about to begin. You might see this happening only for a few seconds, but good pump and dumpers would take their time and do it for hours if not for days. Experienced scammers would proceed with the dumping slowly to avoid creating panic on the market. These performers would begin to sell only small amounts of coins as fast as they can making sure the price is not going down quickly until they sell all their coins. Once the performers are off the market, panic begins and people start selling their coins too. This is the peak time for the dumping process. Both; the price and the volume is now going down, so followers or late joiners begin to realize that their coin is stuck on the market and no one buys them anymore. This is when they panic big time and start to sell their coins below the market value just to get rid of them all. This is also happening because people are afraid that the coin value will drop even more. Once this happens, the coin becomes completely worthless. The scammers, of course are getting out of this at least doubling if not tripling their money. In the meanwhile, the followers losing all their money. Successful scammers might even announce publically that they made a mistake and lost a lot’s of money because someone has scammed them while they are the real scammers. Nobody will know for sure who was running the show behind the curtains or at least at first, but sometimes these scammers just completely disappear from one day to another. They shut down all their social media sites, their websites, deleting their posts from forums and blogs and just move on to the next scam.

If you are capable of spotting a crypto coin that’s getting ready for a pump and dump, you may purchase cheap coins yourself. If you can grab up some coins before the pump starts, you can make money if you’re not greedy and it is not hard to make decent profit in few minutes if you’ve spotted the signs early enough. It is not illegal trade with cryptocurrencies, but if you arrive

late to the party and the coins has already begun dumped but still in the early stages, you still can make a profit. The risk will be bigger and your profit will be smaller but if you enter and walk away fast you should be able to expect a modest profit.

You might also find people offering to participate in such pump and dump games, even offering Bitcoin in exchange. This is illegal and I highly advise you to stay away from such games especially if you are a beginner. Not to mention that some of these scammers go as far as making you believe that they will pump and dump with you, then it might turn out that the only person doing the pump and dump is you. Some might tell you that they will be dumping when the price reaches let's say 5 dollars per token and you might realize that they actually start dumping when the token is actually 4 dollars. I can only advise to stay away from these scammers. Sure, there is a huge potential but you can also lose all your money. Even if you make lots of money on pump and dumps, let me remind you that the only reason you have that money, because many other people lost all their money. Cryptocurrency has its real power in the technology that is based upon. Not scam artists. Pump and dumps are very risky. Even for those experienced in manipulating the market pump and dumps are very risky and illegal. Either if you are a scam coin creator, a pumper, a dumper or a promoter, you will lose your reputation for one, but you might end up paying fines, or worse, those lost their money will sue you and you can easily end up in jail. Instead, spread the word about pump and dump coins and help people not to get scammed. Either way you decide to go about it, there will be wolfs in every market and they always try to leverage on the weak and those are un-experienced on these playgrounds.

Chapter 8 Komodo

Now that we have covered cryptocurrency basics, ICO-s, Pump and dumps and scammers on the market, it’s time to introduce some privacy based cryptocurrencies. First, let me talk about Komodo. The Komodo blockchain is many things. It’s a unique blockchain, a coin that pays interest, a decentralized exchange and a Development blockchain. Essentially it is an end-to-end blockchain solution that external developers can use to build their own blockchains and launch their own ICO-s When external developers build a blockchain on the Komodo platform, they're building their own standalone blockchains. These will also be modular; meaning that these developers and choose the type of features and technologies that they want to include in their blockchain. This all sounds very interesting but what are these features? Firstly you have a decentralized exchange. They've called this the atomic Dex. These utilise atomic swaps and more recently atomic swaps bridge the gap between Bitcoin and Ethereum based blockchains. At its beta release atomic Dex had support for 13 different coins, but can technically support 99% of all existing cryptocurrencies. They also have the “junmblr” feature. This is a cryptocurrency anonymizer developed by Komodo which is decentralized and open source. This uses ZKsnark technology to anonymize transactions and keep addresses safe. Another initial feature of the Komodo white paper was the decentralized fiat currencies and decentralized Initial Coin Offerings. Finally they have their recently launched “Antara framework” This is an adaptable framework for simple end-to-end blockchain development. This will be the framework that will allow for the development of these external blockchains. The framework also comes with built in modules making development speedy and easier. This allows developers to natively support any software DAP or blockchain based games. Now let's take a look at the technology behind the Komodo main change. Interestingly Komodo is a fork of Z cash, which is itself a fork of Bitcoin. So it's built on established technology. Something that I found quite unique about Komodo was their consensus mechanism called “delayed proof of work”. They created a proof-of-work blockchain but modified, it allowing it to recycle bitcoins hash rate to ensure immutability of Komodos blockchain. Komodo does this by using 64 notary nodes that work to notarize blocks in the Bitcoin blockchain. This provides protection for Komodo because an

attacker would have to alter both the Block in the Komodo blockchain and the block in the Bitcoin blockchain. Then on the privacy front, Komodo uses Z cash's privacy enhancing features. More specifically they use zero knowledge proof and ZKsnarks to anonymize transactions. This is "opt-in privacy" which means that users have the choice of sending funds privately or with a regular transparent transaction. Moving on, though let's take a look at Komodos coin. This is the native currency behind the Komodo blockchain and it's called "KMD". This is an interesting cryptocurrency because it also confers holders the right to receive interest. If you hold over 10K MD in your wallet then you'll receive about 5% annual interest on your holdings. The Komodo team has turned this active user reward. The project held in ICO in February of 2017 where they initially sold some of these coins for $0.10 per KMD. Prices have since been on while Wild Ride. In the 2017 bull run komodo coins were trading at an all-time high of over $13 however prices have fallen considerably since then. Although the current value is still above from the ICO price. So it's very much more favourably than many of its other projects that completed in ICO towards the end of 2017. But who is behind the Komodo project? Well, initially the Komodo founders and core team kept things pretty private and new pseudonyms. But as the project has grown the team has been more transparent with their identities. The full team is now nearly 30 members spanning leadership, development, marketing and community development. Speaking of community, there are numerous contributors from the community both; developers and community outreach ambassadors. The Komodo developers appear to have been pretty active as well. This can be verified by their github activity. In fact when compared to their peers, Komodo is ranked 30th in terms of commits and 12th for overall coding activity so it's pretty impressive. What do the markets look like for the Komodo coin? Well, pretty robust actually. KMD is listed on a number of exchanges including Binance, Bittrex and others. The volumes are also pretty well spread out across these exchanges and there is a reasonable turnover on these exchange books. This implies that there are healthy levels of liquidity and hence easy order execution. When it comes to offline storage you have a rather limited selection of wallets. Perhaps your best bet is their native Komodo Ocean QT wallet. Komodo developing a relatively sophisticated blockchain platform and ecosystem. One that not only makes blockchain development effortless but also uses unique privacy and security enhancing technology. The KMD coin has also been a better format than most other

projects that raised funding in 2017. Yet there are challenges. They have a lot of competing blockchains and ecosystems that developing similar technology. These include numerous decks based coins, developer blockchains and privacy focused coins. None of them have really combined it all into one solution but there is the risk that their laser focused approach could trump Komodo's or encompassing one. So it'll be interesting to see how things play out in the coming years.

In terms of the price, Komodo started trading around 11 cents a coin and it reached its all-time high close to 13 dollars per coin. This means that if you have invested at the time of its all time low and would sold off at its all-time high price you would have gained a 118X. As an example, you could have potentially made $11,800 on $100 investment. To learn more about Komodo, please visit the following website:

https://coinmarketcap.com/currencies/komodo/

Here you find additional links to Komodo's website, Explorers, Source Code, technical documentation, historical data, on-chain Analysis and charts for market capitalization and price.

Chapter 9 DeepOnion

DeepOnion is another anonymous cryptocurrency integrated with TOR network, also known as The Onion Router. The platform works with proof of stake and the x13 proof of work algorithm, using its brand-new cryptocurrency called ONION. By developing an untraceable payment platform, the firm aims to protect individual's privacy, security, and identity. The platform is expected to avoid legal or illegal identification of cryptography network protocol. The cryptocurrency "ONION" coin is listed on few of the leading cryptocurrency exchange including Kucoin, Stock.Exchange, Cryptotopia and a few more. Besides trading access through secure exchanges, DeepOnion has its own wallet which can be downloaded for Windows, Mac or Linux. DeepOnion plans to implement innovative blockchain technologies, called DeepSend which enables tracking the coin flow within the DeepOnion network. Moreover, an ONION coin holder will have a secure platform to transfer the funds without the fear of uncertainty and malicious attackers. They claim that a user can quickly send and receive private transactions using the DeepOnion wallet.

In terms of the price, DeepOnion started trading around 11 cents a coin and it reached its all-time high close to 18 dollars per coin. This means that if you have invested at the time of its all-time low and would sold off at its all-time high price you would have gained a 163X. As an example, you could have potentially made $16,300 on $100 investment. To learn more about DeepOnion, please visit the following website:

https://coinmarketcap.com/currencies/deeponion/

Here you find additional links to DeepOnion's website, Explorers, Source Code, technical documentation, historical data, on-chain Analysis and charts for market capitalization and price.

Chapter 10 Solaris

Solaris also is a type of cryptocurrency that works on the principle of decentralization and fair distribution. Solaris uses NIST5 and Proof of Work algorithm, and the network provides a secure setting for people to make transactions. The anonymity of users also provides a sense of privacy as people go about their transactions. Users are in a position to send and receive coins worldwide without fear that their identities will be revealed. The transactions fees incurred are very little and also when Solaris is exchanged for other cryptocurrencies, miners do not charge transaction fees as they are reimbursed by the network.

In terms of the price, Solaris started trading around 37 cents a coin and it reached its all-time high close to 49 dollars per coin. This means that if you have invested at the time of its all time low and would sold off at its all-time high price you would have gained a 132X. As an example, you could have potentially made $13,200 on $100 investment. To learn more about Solaris, please visit the following website:

https://coinmarketcap.com/currencies/solaris/

Here you find additional links to Solaris's website, Explorers, Source Code, technical documentation, historical data, on-chain Analysis and charts for market capitalization and price.

Chapter 11 Sumokoin

Sumokoin has been launched in May 2017, and it's a fork of Monero, which I am going to talk about later. Sumokoin Coin is based on the CryptoNote protocol instead of blockchain. What it does is basically places more importance on security, privatization and non-traceability than other cryptocurrencies, such as blockchain based cryptocurrencies. Sumokoin can be mined by anyone and their currency symbol is SUMO. Sumocoin wallet can be downloaded to windows, mac as well to Linux, and you can find it on exchanges like Cryptopia or Livecoin.

In terms of the price, Sumokoin started trading around 4 cents a coin and it reached its all-time high close to 11 dollars per coin. This means that if you have invested at the time of its all time low and would sold off at its all-time high price you would have gained a 275X. As an example, you could have potentially made $27,500 on $100 investment. To learn more about Sumokoin, please visit the following website:

https://coinmarketcap.com/currencies/sumokoin/

Here you find additional links to Sumokoin's website, Explorers, Source Code, technical documentation, historical data, on-chain Analysis and charts for market capitalization and price.

Chapter 12 Firo aka Zcoin

Firo used to be known as Zcoin or Zerocoin is an open source decentralized cryptocurrency that focuses on achieving privacy and anonymity for its users while transacting. Zcoin is a privacy focused crypto currency that allows people to transact anonymously in a unique and scalable way. Up until very recently, Z coin utilized the “0 coin protocol”. This protocol was originally built as an extension of Bitcoin. However in July of 2019 they released their Sigma protocol. This makes use of much more advanced technology in cryptography. The privacy coin sector is quite saturated at the moment so how can Zcoin really differentiate itself? Well, in order to get a better sense of that, we have to take a look into the technology. Zcoin was built on the “0 coin protocol” which was a pretty unique way to approach privacy. Previously the “0 coin protocol” involved destroying Zcoins to mint “0 coins”. These were coins with no transaction history. The protocol worked as a sort of coin laundry, where you'd exchange your existing “dirty coins” those were the transaction history, for new clean coins which had no transaction history at all. This process of creating new coins is called “minting”. This “0 coin protocol” was a logic start for Zcoin but it did not come without some baggage. First of all the “0 coin protocol” was built on something called a “trusted setup”. This is something that is relied on by other cryptocurrencies such as Zcash and can be seen as a single point of failure. Essentially, with the trusted setup you have to have a trust and as we know from the Bitcoin mantra; “don't trust, verify”. Another serious problem with the “0 coin protocol” is that it had a number of vulnerabilities. These vulnerabilities allowed an attacker to create forged Zcoins. This happened on two occasions. Once in 2017 and then again in 2019. This led to over 1% of the circulating supply being forged. Not an insignificant number. So it was these events that forced the developers to come up with an alternative protocol and hence the release of “Sigma”. Sigma has a number of benefits over 0 coin, but perhaps the most important is that it does not have the trusted setup or the fatal flaws. This has been running effectively on the main net and the initial results appear to be quite positive. Let's move off of the core protocol and on to the other features of the blockchain. Something else that I liked about Zcoin is that it uses a hybrid consensus mechanism. It has a proof-of-work component which means that you can mine it. Yet it also has a proof of state component

which means that you can earn returns by staking your coins. Essentially if you put up 1,000 Zcoin, you'll be able to run as equine masternode called as “z node”. Z nodes are incentivized by receiving 30% of the newly minted Zcoins. To put that into context at current prices and difficulty its return of about 15.3%. On the mining component, Zcoin uses the MTP algorithm. You can actually still mine Zcoin on a GPU although it is becoming that much more difficult. Something that you have to be aware of when you mind Zcoin is that they have what is called the “founders fund”. With this a certain percentage of the mining reward will go to the founder investors and the team. This can seem unfair to some but it's a system that is used on larger privacy blockchains such as Zcash too. Moreover, this will only continue until September 2021, at which point it will be fully funded. Moving on something else that worth look at is their combination of Tor integration and the “dandelion” protocol. This is something that adds a further layer of privacy to Zcoin transactions. Essentially with these features the IP address of the sender is masked from the broader network. This means that not only are your transactions private but no one will be able to see that you have even connected to the Zcoin network. This is not a feature that is built into many other privacy coins, although you have a similar protocol on Verge. The dandelion protocol further advances this anonymity functionality. Another central piece of the Zcoin network is their native coin. This has the ticket of XZC and was released back in 2016 with no pre mine coins or ICO. Given that it's based on the Bitcoin protocol it has a maximum coin supply of only 21 million 0 coins. The price of this coin has been all over the show during the 2017 bull run we saw all-time highs of a 169 dollars but when the bear market came rolling in, prices kept rolling down. Who is behind this project? Well, the team behind Zcoin is quite experienced. The developers are also hard at work. Something that you can verify yourself by checking out their github repository. Finally, there are also some high-profile investors behind the project. The most prominent of these has to be Roger Ver, who invested in the project in its early stages. Zcoin is listed on a number of exchanges including MXC, CoinX, Binance and so on. In terms of volume, the top three exchanges control over 85% of it so it’s slightly concentrated. There appears to be reasonable levels of liquidity on most exchanges. For example the Zcoin, Bitcoin ordered books on Finance are deep and have decent turnover levels. In terms of storage, your best bet is probably to use the official Zcoin desktop wallet. If you're looking to store it on mobile, then you could use the

Edge wallet. The project is pretty well established and includes a number of unique features not seen on other privacy coins. They've also recently shed the 0 coin protocol which was the source of much concern around the safety of Zcoin. The developers also appear to be quite competent, motivated and are actively pushing out code at a wild pace. There are also some really interesting updates that we can look forward to in their roadmap. Having said all of this, there are potential bumps in the road ahead. Firstly, it's still early days on their segment protocol. You also have an increasingly saturated market for privacy coins. The market may be slightly jaded by the plethora of projects occupying the space. Finally that Z coin price is still quite depressing. This is not only impacting the value of the portfolio but it's also reducing the potential return for Znode operators.

In terms of the price, Zcoin started trading around 40 cents a coin and it reached its all-time high close to 169 dollars per coin. This means that if you have invested at the time of its all time low and would sold off at its all-time high price you would have gained a 320X. As an example, you could have potentially made $32,000 on $100 investment. To learn more about Zcoin, please visit the following website:

https://coinmarketcap.com/currencies/firo/

Here you find additional links to Zcoin's or Firo's website, Explorers, Source Code, technical documentation, historical data, on-chain Analysis and charts for market capitalization and price.

Chapter 13 AEON

Aeon is Monero's little brother and was introduced in June 2015. It is also based on the CryptoNight algorithm and it's purpose is to be a lightweight version of Monero. Aeon has true anonymity & data protection. By default, Aeon utilizes a cryptographic system to transfer funds without the identifying information of each user becoming visible. Aeon uses ring signatures to make transactions untraceable, meaning it is very difficult for anyone to determine if funds have been spent. Basically it creates un-linkable transactions with random data by the sender. Each transaction is secured with robust cryptography, and distributed through a global peer-to-peer consensus network. Aeon can be mined by anyone as well using CPU or GPU.

In terms of the price, Aeon started trading around 009 cents a coin and it reached its all-time high close to 9 dollars per coin. This means that if you have invested at the time of its all time low and would sold off at its all-time high price you would have gained a 118X. As an example, you could have potentially made $100,000 on $100 investment. To learn more about Aeon, please visit the following website:

https://coinmarketcap.com/currencies/aeon/

Here you find additional links to Aeon's website, Explorers, Source Code, technical documentation, historical data, on-chain Analysis and charts for market capitalization and price.

Chapter 14 Bytecoin

Bytecoin is a private, decentralized cryptocurrency with open source code that allows everyone to take part in the Bytecoin network development. Privacy and security come naturally from using Bytecoin. They claim that Bytecoin is the best solution for those who want to keep their financial privacy. Instant private transactions are provided all around the world by the Bytecoin Network. They are totally untraceable, and they don't require any additional fees. According to the company, Bytecoins are gradually getting more expensive over time, since the production is limited to 184.47 billion bytecoins. The number of Bytecoin emitted each 120 seconds is slightly decreasing. As a result BCN gains value and the exchange rate increases.

In terms of the price, Bytecoin started trading around 0.000065 cents a coin and it reached its all-time high close to 0.015 per coin. This means that if you have invested at the time of its all time low and would sold off at its all-time high price you would have gained a 230X. As an example, you could have potentially made $23,000 on $100 investment. To learn more about Bytecoin, please visit the following website:

https://coinmarketcap.com/currencies/bytecoin-bcn/

Here you find additional links to Bytecoin's website, Explorers, Source Code, technical documentation, historical data, on-chain Analysis and charts for market capitalization and price.

Chapter 15 Navcoin

Navcoin is a community driven project that was launched back in 2014 so they're quite established for a cryptocurrency. The team is trying to develop a cryptocurrency that is simple to use, scalable and private. It was built from the Bitcoin core code but there are several changes that were implemented. For example they did away with Bitcoin's proof-of-work consensus algorithm and moved to proof of stake. They also launched a sub chain called Navtech which enabled mixing and anonymization of the transactions. So let's take a closer look at this technology. Given that Navcoin has moved to a different consensus method, they are able to process transactions much more quickly. For example, Navcoin has a block confirmation every 20 seconds compared to the ten-minute block time for Bitcoin. Apart from the speed, you also have reduced transaction costs and increased scalability. This is particularly relevant today where bloated blockchains cause a whole host of problems. On top of this the Navcoin community has approved the activation of segwit and they are looking to implement an off chain solution similar to the Lightning Network. When it comes to their privacy tech solution Navcoin has an opt-in privacy feature. This means that transactions are public by default but users can elect a mix and encrypt their transaction with the nav tech sub chain. Navcoin is also working on their "Valence" project. This plans to use the nav check sub chain to add different types of function with the first being the addition of an autonomous platform for decentralized applications for daps.

"Nav" is the native coin that is used on the Navcoin ecosystem. This was released without any ICO or pre mine which should make it more decentralized in theory, however there is a relatively small subset of wallets that seem to control the bulk of the coin supply. The company behind Navcoin is called Encrypt S Limited and their base in New Zealand along with the founder and lead developer. Apart from this, the project is completely community run. In fact Navcoin even has a community fund that is used to pay for project improvement. It's topped up by 0.5 Nav per block mind which is about half a million Nav per year. Coin users can submit proposals and vote on these initiatives so the network really does decide. In terms of trading, Nav is listed on a few different exchanges but the bulk of the volume is being done on Binance. Even then there is not that much

turnover on the exchange. This implies lower levels of liquidity and hence a chance of slippage with large orders. Given that the Nav cone is a native cryptocurrency there are not too many wallets that you can use for storage. If you want to earn staking returns and you'll probably want to download and install their Navcore wallet. Though, if you would like to just store them in a third party PC wallet then you can use Koyomi. In conclusion, Navcoin is quite an established cryptocurrency that has stood the test of time. I like the fact that it's a community driven project and that there was no ICO or pre mine. They've also focused on a key point for the legacy blockchain which is scaling. There are many other projects trying to build scaling solutions for superfast blockchains so there needs to be more awareness for the project if they want to stand out from the crowd.

In terms of the price, NavCoin started trading around 0.004 cents a coin and it reached its all-time high close to 4 dollars per coin. This means that if you have invested at the time of its all time low and would sold off at its all-time high price you would have gained a 1000X. As an example, you could have potentially made $100,000 on $100 investment. To learn more about NavCoin, please visit the following website:

https://coinmarketcap.com/currencies/nav-coin/

Here you find additional links to NavCoin’s website, Explorers, Source Code, technical documentation, historical data, on-chain Analysis and charts for market capitalization and price.

Chapter 16 PIVX

PIVX is also a privacy based coin which stands for Private Instant Verified Transaction. PIVX first was called Dark Net; but it has been re-branded in January 2017. PIVX block time is 60 seconds and the total supply that ever be on the market is 43 million PIVX coin. PIVX has a really nice community, and its always very good to have supporters, thus for the coin to take off you will need lot's of followers and many admires which PIVX has. Additionally to their community, PIVX has an excellent looking website, and their marketing strategy is also unique. PIVX has multiple forums, YouTube channel, Twitter account, however more importantly a constructive community. This is vital. If you have any questions you can get a quick reply, which not only helpful but the way they reply always makes sense in terms of the quality answer. Some of those projects where you don't get a reply for your question or the answer is not clear; I highly recommend to stay away from. The algorithm that PIVX uses is called: Quark. Additionally to Quark algorithm, PIVX applies proof of steak 2.0. PIVX has been build up as a fork of Dash, with a little mixture of Bitcoin Core; therefore it's a fascinating hybrid technology. PIVX has started off back in January 2017 when they also created their wallet software but they also have been building many more exciting features. Such features are called Multi Signature Access Control and Multi Sig Escrow system. PIVX also offers SWIFT Transactions which confirms transactions in seconds guaranteed by the master nodes without having to wait for multiple confirmations for validity. Basically all it means that PIVX transactions are lot faster than Bitcoin. Another great feature is that they have managed to have a built-in Encrypted Chat system to their wallets, which is something that no other cryptocurrency company has ever achieved, especially within privacy based coins.

In terms of the price, Kom PIVX odo started trading around 10 cents a coin and it reached its all-time high close to 13 dollars per coin. This means that if you have invested at the time of its all time low and would sold off at its all-time high price you would have gained a 130X. As an example, you could have potentially made $13,000 on $100 investment. To learn more about PIVX, please visit the following website:

https://coinmarketcap.com/currencies/pivx/

Here you find additional links to PIVX’s website, Explorers, Source Code, technical documentation, historical data, on-chain Analysis and charts for market capitalization and price.

Chapter 17 DASH

The crypto space is growing and not just in terms of market cap. There over 7600 cryptocurrencies currently in existence. Just a few years ago there were only a few hundred. One of the OG coins that are still around today is Dash. Since its born in January 2014, Dash has remained one of the highest ranked coins by market cap. This is quite impressive given the relentless competition it and many other veteran crypto projects like Ethereum have faced since their inception. This intense competition might be what prompted Dash to pivot significantly in its mission. Dash's transformation was not sudden; in fact it's been in the works for a long time. What has changed, what will change and how will dash's evolution impact the future of this former top 5 token? Well, let’s take a closer look. Dash stands for Digital Cash and it's a fork of Bitcoin which focuses on speed and until recently, privacy. Dash is also considered to be one of the first and one of the longest running decentralized autonomous organizations. This is due to its use of decentralized master node network which can vote on proposed changes to Dash. Dash was created by software developer Evan Duffield who was the CEO of Dash core group until 2017 when he stepped into the background of the project as an advisor. Dash core group is the company contracted by the Dash Dao to maintain and develop Dash. The Dash Dao also funds Dash's marketing operations branch called Dash newsroom and an investment fund called the Dash Investment Foundation which provides loans and funding to companies looking to incorporate Dash into their business operations. Dash seeks to be what Bitcoin was supposed to be, a peer-to-peer electronic cash system but there are a few differences. First, Dash is much faster than Bitcoin. Dash can process around 56 transactions per second versus Bitcoin; seven. In practice, it takes less than two seconds for a Dash transaction to complete. This is magnitudes faster than Bitcoin's 10 minute transaction time which can turn into hours when the network is busy. Second, Dash is much cheaper to send than Bitcoin. Transaction fees on the Dash blockchain are less than a cent, whereas Bitcoin transactions cost a few dollars on a good day. Third, Dash gives users the opportunity to easily send a private transaction using privatesend which is their own in-house version of coin-join, a privacy protocol originally developed for Bitcoin. These characteristics are pretty legit so it should come as no surprise that Dash has

consequently seen considerable adoption. There are over 2000 Dash ATMs around the world. Over 5000 merchants accept Dash as a form of payment. Dash processes over 20000 transactions per day and has moved nearly a billion dollars' worth of currency since its release. Most of Dash's traffic is coming from Latin America and especially Venezuela where over 2500 merchants accept Dash. Venezuela has been going through some dark economic times and runaway inflation has Venezuelans turning to Bitcoin and Dash as an alternative to bolivar feared. You may have heard about Venezuelans using Bitcoin in the news apparently the use of Dash is just as common. Dash also recently partnered with Mexican cryptocurrency exchange Touros.io to release the first Latin American visa debit card backed by cryptocurrency. You can also use Dash to pay for hotels on trivaga.com. Despite all these impressive numbers, Dash appears to be tumbling down the rankings and the project has lost a lot of social steam. Dash has been in the crosshairs of regulators ever since its release and this may be a large part of why the project has struggled to regain its former glory. For starters, Dash got in a battle with the Securities and Exchange Commission of the United States in 2018. The SEC was probing cryptocurrency exchanges, asking them whether they thought Dash should be classified as a security or not. If classified as a security, Dash would be subject to some pretty heavy-handed regulations. Dash core group CEO Ryan Taylor subsequently flew out to Washington DC to speak in person with members of the SEC to explain to them that Dash was not a security. This was because there was no ICO for Dash and there was no centralized issuer of the Dash cryptocurrency. This puts it in the same category as Bitcoin which fails the "how we test" used to determine whether an asset is a security or not. After trying multiple questions on Ryan, the SEC took Dash off its radar and has not inquired about it since. Holders of Dash must certainly have been nervous in the months that followed that meeting. Dash is actually the project's third name. The first name X coin, was scrapped during the first month of the coin's release. The second name Darkcoin, was changed after multiple cryptocurrency exchanges refused to list Darkcoin. To the untrained eye, Darkcoin looks like the "baddest boy" on the crypto block. That image has continued to haunt the project even though it renamed to Dash and rebranded to a professional digital currency in 2015. Dash has been repeatedly put up with the same category as other privacy coins like Monero and Zcash. This has consequently landed it the same treatment. To give a few examples Dash

was delisted on south Korean cryptocurrency exchange OKEx along with Monero and Zcash in September 2019. In October 2019, Japanese regulators described Dash, Monero and Zcash as “three anonymous siblings”. In October 2020, the United States Department of Justice published an enforcement framework for cryptocurrency which included Dash in its list of anonymity-enhanced cryptocurrencies and stated that the use of these cryptocurrencies is “indicative of possible criminal conduct”. Is all of this justified? Well, no. To understand the reason why, we just need to look at Dash's private send feature which makes transactions anonymous. As mentioned earlier private send is basically just a branded version of coin-join. Both involve mixing multiple transactions together, so that it becomes nearly impossible to figure out who is sending money to whom. The main takeaway here is that coin-join is available to Bitcoin users in the same way that private send is available to Dash users although with a few extra clicks. In other words, privacy is not built into the Dash blockchain itself like it is with other privacy coins like Monero and Zcash. This has been the argument tabled by the Dash core team which has spent a great deal of their time trying to educate regulators. Dash is more similar to Bitcoin than it is to privacy coins. Still, you might be wondering how often people are using Dash's private send feature. Well, according to analysis only 0.7 of Dash transactions involved the transfer of funds were made using private send. Also a smaller and smaller percentage of Dash transactions involve private send as time goes on. This means that of the 700 million USD which has been transacted on the dash network, only about 5 million US dollars of possible criminal conduct has occurred using Dash in almost 7 years. A report by the 1000x Group released in February 2020, did not list Dash as one of the cryptocurrencies used in criminal activities. In fact Dash is not even accepted as a form of payment on any major Darknet marketplace according to various reports. This has certainly had an impact on the project's ability to grow and compete. Another big reason why Dash has been struggling is universal in the crypto space competition. Dash is probably second or third in the areas it's competing, namely payments and privacy. If you want to be a cryptocurrency payments provider, you need to be able to scale. While Dash may offer a two second transaction time, Dash can only process about 56 transactions per second. Credit card companies such as Visa can process 1700 transactions per second and something like that will be needed if Dash wants to provide reliable payment services to a significant amount of people. Meanwhile, new

next generation blockchains such as Solana are pushing 65000 transactions per second. Even layer 2 solutions for Ethereum like “Loop ring” can now process over 2000 transactions per second and Loop ring pay makes it possible to send more stable Ethereum based assets such as USDT at an even cheaper price and faster speed than Dash. The average retail investor would prefer to count in US dollar stable coins than decimals of comparatively volatile Dash tokens. Finally, even though Dash has managed to gain somewhat of a foothold in Latin America, a Dow funded cryptocurrency project will have a hard time competing with Binance in the crypto debit card and payment space. Regarding privacy in early October 2020, a representative from the Dash core team stated that Dash should not be considered a privacy coin. This might by a surprise for some but this is technically correct. The problem is that Dash's privacy element was one of the major selling points of the project, perhaps even more so than the payments element. More importantly, competition in the privacy coin space is not nearly as intense as in the payment space. There are only about 100 privacy coins out there and most of them have sprung up in the last few years. While most of them are probably write-offs, some of them offer next-level privacy tech such as Monero for example. Another privacy coin which has emerged in recent years is called PIVX. PIVX was apparently founded by a group of disenfranchised dash developers in 2016, who thought dash had betrayed its privacy roots. In addition to members of the Dash core team shying away from privacy during interviews in recent years, the original Dash white paper is titled “Dash: A privacy-centric cryptocurrency”. Dash notes on its website that the white paper should be considered a historical document. If they embrace their privacy angle, they'll get severely restricted by the regulators. If they abandon privacy and go all in on the payments, they'll get crushed by the competition. Nevertheless to the cryptocurrency community at large, the Dash core team had a third option hidden up their sleeve. The Dash platform is a layer 2 smart contract network powered by Dash master nodes. The Dash platform was first proposed in 2015 by Dash's original creator Evan Duffield under name “Evolution”. A white paper for Evolution was published by the Dash core group in 2017 and the test net for the renamed Dash platform finally launched in December 2019. The Dash platform consists of four key elements. The first is a “dappi” short for Decentralized API which will be the world's first Decentralized HTTPS API. The second is the Dash drive which is a decentralized cloud storage system to

store data from decentralized applications built on the Dash platform. The third is the Dash platform name service or DPNS which turns Dash wallet addresses into human readable usernames to make transactions easier. The fourth is the Dash platform protocol. The first three are fairly self-explanatory. The Dash platform protocol needs a bit more explaining but it's still currently in development and information about it is pretty limited. All Dash is doing is adding a layer to blockchain which supports smart contracts like Ethereum and Polkadot. What's next for Dash? Well, development of the Dash platform testnet is on-going and seems to be quite aggressive. The Dash core team stated in April 2020 that they'll be updating the test net every six weeks until they're satisfied. No specific date has been set for the main net launch of the Dash platform. The Dash roadmap notes a series of milestones the Dash core team is hoping to accomplish before the end of 2020. These include giving incentives to master nodes to host and service the Dash platform, making it possible for light clients such as mobile devices to connect to the Dash platform, and introducing Dash pay which will function as a sort of hub for the Dash platform. Dash has also been very aggressive with marketing in Latin America where adoption seems to be growing. Dash core CEO Ryan Taylor noted that they're employing a strategy like Visa in its early days, focusing all their attention on a single market. Beyond that, the future of Dash will be guided by the votes from its master nodes as has been seen since 2015. While the project seems to have lost some momentum, the decisions of the Dash community have carried the project for seven years and most probably they will carry it for many more. Dash is many things. For some, Dash is an investment vehicle, for others Dash is the means by which they live in the face of broken or absent centralized financial infrastructures. And for the select few, Dash is the perfect to justify overreaching regulations of a new decentralized monetary system and asset class. Dash is not a privacy coin. All it does, is give users the option to use a privacy technology which is also available to Bitcoin and many other Bitcoin-based cryptocurrencies. Privacy is not built into Dash like Zcash or Monero. Dash is not even accepted as a form of payment by major dark net marketplaces. Despite these facts, constant scrutiny from ill-informed government regulators and dense cryptocurrency exchange gatekeepers have arguably held Dash back in its development and growth for years. This left Dash with a dilemma; double down on its privacy focus and face repercussions, or attempt to face off against decentralized and centralized titans in a hyper-competitive payment

space. Instead, Dash has chosen a third part, one which has been under construction for half a decade. Rather than fight for territory in the payment space, it's creating its own territory with the smart contract-enabled Dash platform. With some luck, Dash will get enough traction in its Latin American niches to begin expanding to other markets. This might just bring it back to its all-time highs.

In terms of the price, Dash started trading around 20 cents a coin and it reached its all-time high close to 1500 dollars per coin. This means that if you have invested at the time of its all time low and would sold off at its all-time high price you would have gained a 7500X. As an example, you could have potentially made $750,000 on $100 investment. To learn more about Dash, please visit the following website:

https://coinmarketcap.com/currencies/dash/

Here you find additional links to Dash’s website, Explorers, Source Code, technical documentation, historical data, on-chain Analysis and charts for market capitalization and price.

Chapter 18 Zcash

Zcash is one of the most well-known privacy coins on the market. It is also one of the oldest. It was built on the original Bitcoin codebase. The Bitcoin fork that became Zcash occurred in 2016, resulting in a coin specifically designed to provide anonymous transactions. The team behind Zcash wanted a private and fungible option within the crypto community. A region called “zero cash” the project was eventually renamed Zcash. Like other digital coins, you can use Zcash to purchase products and services, or you can trade it for other types of money. This includes Euros, US dollars or any other type of fiat currency that you prefer to use. But unlike other privacy coins, Zcash allows you to control exactly what you want to share. You can shield your address so that it's not viewable on the network, or you can provide access to payments and transactions to trusted third parties. Zcash also has some well-known proponents including the likes of Edward Snowed. He said “Zcash's privacy tech makes it the most interesting Bitcoin alternative. Bitcoin is great, but if it's not private it's not safe.” The Zcash project has key features that it believes will appeal to users looking for a viable privacy coin. First, Zcash is efficient and usable. It's reliable, fast, inexpensive and is supported by many wallets and exchanges. Next, Zcash is regulation and audit friendly. This means private transactions and addresses can be shown to third parties and auditors in an effort to comply with regulations and requirements. Thirdly, its attack resistant and decentralized. Zcash is maintained and operated by a wide network of machines and people. There's no single point of failure or centralized database vulnerability to hacks. Lastly, Zcash offers private transactions and addresses. Privacy resides at the core of the Z cash project. This means that you can send and receive transactions without allowing people to view where it was going or how much was sent. How does this privacy coin work? Well, to dive deeper into how Zcash transactions work, you will need to have a solid understanding of how Bitcoin transactions take place. Let's say you send me one Bitcoin to my wallet address. In doing so you'll sign the transaction with your private key. That transaction heads to the Bitcoin blockchain, where miners put it into their blocks. When the block is propagated the transaction is confirmed. As a result the network is updated and the transaction is stored. Unable to be changed, and most importantly it’s completely public. So how is Zcash's own privacy transaction different?

Well, the transaction will be pretty much the same if I ask you to send me Zcash to my address. That's my transparent address, however if we wanted to make the transaction completely private, then I would give you “Z address” or “stealth address”. Once you send Zcash to this address, the transaction is kept completely anonymous. All information about the sender, receiver and amount is hidden from those prying eyes. The tech behind these stealth transactions is pretty advanced. To validate that a person has the necessary funds to send a certain amount of Zcash, the network uses ZKsnarks. ZKsnarks is a protocol used to validate that nobody on the network is stealing or cheating. These ZKsnarks or zero knowledge proof are used to verify that a person on the network has a secret. In this case the private key but won't reveal what the secret is. ZKsnark actually stands for zero knowledge succinct non-interactive argument of knowledge. This refers to the cryptographic proof where one can establish possession of information without revealing what the information actually is. It can also confirm this information without interaction between the verifier and the prover. Zcash isn't the only project using the ZKsnarks protocol. There are several others that have implemented this type of technology. For example you have Komodo which is a multifunctional blockchain that's looking for a way to shield their transactions. You also have Horizon, which has ZKsnarks technology and pretty much the whole Zcash codebase. Horizon is actually a fork of Z Classic which is a fork of Zcash. When it comes to consensus, Zcash uses proof of work just like Bitcoin. This means coins are mind through the use of raw computing power. Through the use of hashing, miners solve complex algorithms to earn rewards for a mind block. Both Bitcoin and Zcash have a total coin supply of 21 million coins. However Bitcoin uses a SHA-256 hashing function while Zcash went the “Equihash” route. As a result, Zcash is much easier to mine than Bitcoin. You used to be able to mine Zcash with the GPU but this has become unprofitable on account of all those echo hash ASIC mining rigs that are on the market. If you have an Equihash ASIC, then you may want to link it up to Zcash mining pool. Zcash launched through an elaborate event called the trusted ceremony. this was essentially the point where the initial Snark public parameters were created. There are many privacy people didn't like the notion of the ceremony. They were sceptical as it relied on the trust of the founding members. As we know in crypto, don't trust, verify. ZCash was founded in 2016 in a period when the very first AI were getting underway. Zcash chose not to have one instead

going in a direction it refers to as the “founders reward”. The founders reward is the incentive mechanism used by the project for the founders and early investors. They received 10% of all mining rewards which will wind up being roughly 2.1 million “Zec” over the course of a four year period. Once this four-year period elapses, the block reward is only split among the miners. As is the case with most other proof-of-work coins. Zcash has a total my noble supply of 21 million coins. Currently there are just under eight million Zec coins in total supply and circulation. Zcash also experienced a halving in 2020 as well. At the time, miners receive 12.5 Zec per block mined which will halved to 6.25 Zec. The Zcash team is led by Zuko Wilcox who founded the project in 2016. Zuko currently serves as the CEO with a solid background in decentralized systems and cryptography. Previous endeavours include Digit cash and Mojo nation. While Zcash is an open-source project, the team works for “0 coin electronic” company. This is a registered company that does the development work for the Zcash project. Zcash also boasts a strong advisory board included amongst the Zcash projects backers are Roger Ver, Erik Voorhees and Barry Silbert. The project is doing some significant work as evidenced by its upgrade. This network upgrade took place in October of 2018 and provided significant improvements to the project. “Sapling” introduced shield addresses to Zcash which helps reduce the time of constructing transactions while also reducing the amount of memory required. Zcash which has the ticket ZEC is a pretty popular coin and consistently ranks within the top 50 of all cryptocurrencies on CoinMarketCap. You won't have any problems with liquidity when it comes to Zcash. There's plenty of volume done each day on exchanges like CoinEX or Binance. These platforms do literally millions in Zcash trading on a daily basis. The trading volume is also pretty well spread out across these exchanges which is better from a price discovery perspective. Taking a bit of a closer look into the exchange order books, we can see healthy liquidity. In terms of storage, Zcash has plenty of options. Privacy should be a human right and in a world of ever-increasing surveillance, we are losing that. Our Bitcoin was a first step in this direction. It's a completely public blockchain and it has proven to be a massive asset for those who want to track your transactions. Well Zcash is one of the oldest on the market and it is constantly innovating. It has a strong team behind it with broad exchange support. Moreover, the technology that powers the Zcash protocol is some of the most advanced in the cryptocurrency space. The numerous new cache Forks are

testament to that. Finally Zcash is really likely to blossom with its upcoming upgrade. But, there are a few concerns with Zcash. Firstly it is opt-in privacy. Unlike other privacy coins like Monero where all transactions are private by default, Zcash require the users to select to send a private transaction. This means that those who use shielded transactions are immediately viewed with suspicion as having something to hide. So those who use transparent transactions are lessening the privacy of those who use the shielded transactions. Secondly, you have that trusted ceremony. While the chances of the ceremony being compromised are incredibly low, the possibility still exists. Some may not be bothered by this but others would be highly worried.

In terms of the price, Zcash started trading around $34 a coin and it reached its all-time high close to 704 dollars per coin. This means that if you have invested at the time of its all time low and would sold off at its all-time high price you would have gained a 20X. As an example, you could have potentially made $2,000 on $100 investment. To learn more about Zcash, please visit the following website:

https://coinmarketcap.com/currencies/zcash/

Here you find additional links to Zcash's website, Explorers, Source Code, technical documentation, historical data, on-chain Analysis and charts for market capitalization and price.

Chapter 19 Monero

The Bitcoin blockchain is revolutionary. A decentralized censorship resistant and transparent ledger of value but that transparency is also one of its biggest flaws. Every single transaction and wallet balance is visible to everyone; the government, hackers or you're jealous ex, everyone. Monero it's a peer-to-

peer digital cash that was developed specifically for privacy. Given the untraceable nature of its blockchain, it's perhaps the closest that you will get to a fully anonymous cryptocurrency. Isn't Bitcoin anonymous? Well, no, it's not. While your name is not on your Bitcoin address, everything else about this address is visible. Hence, all someone needs to do is connect your name to this address. With Monero, this cannot be achieved. Even if you had someone's public address you could not observe its balance. You cannot trace transactions. Its units are completely fungible. The term fungible means that a currency is identical and mutually interchangeable with another unit of the same currency. Two separate Moneros cannot be distinguished. But Bitcoin bought on web is not equivalent to the one you bought on Coinbase. How effective is Monero? Well is probably viewed as crypto enemy number one by numerous regulatory agencies. So it’s pretty effective. Monero was built on the crypto note protocol and was launched back in 2014. It was born out of a disagreement with a developer and the broader community. There are two key components that allow Monero to keep its blockchain hidden. These are stealth addresses and ring signatures. With a stealth address, Monero allows a sender to create a one-time public address for every single transaction on behalf of the recipient. But the recipient can still use a single address that receives all incoming payments. Basically when you get started on Monero, you'll generate a private view key, a private spend key and a public address. As the name suggests the spend key is used to make payments, the view key will be used to signal for incoming transactions coming to your account. That public address is for receiving all incoming transactions just like a Bitcoin address. Ring signatures is a concept that is used in general cryptography. It's essentially a signature that can be signed by any member of a group of people who have private keys. But a key feature of a ring signature is that it's impossible to determine whose key was used to sign, so it provides that anonymity. Monero has implemented these ring signatures into their transaction protocol. It'll make use of your private key along with a ring of possible other signers on the network. Because ring signatures give anonymity to the signer, no one can determine which signature is that of the true account. This is a relatively simple explanation. What does this all mean for the Monero user? Well, it means that you can freely share your Monero public address with whoever you want. You can receive payments into that address as many times as you want. But no one can see what you hold or when you transact. All hidden from prying eyes.

There is another really important point to make here and that is that all transactions are private. It's not an opt-in feature. All Network participants on Monero helped to uphold the privacy of everyone else. This is unlike other well-known privacy coins like Zcash which have made this feature; opt-in. There are pros and cons to each approach. Just like Bitcoin, Monero is a proof-of-work cryptocurrency which means that it is minable. Up until very recently, it used to use the “crypto knight” hashing algorithm but since the 30th of November 2019 there was an upgrade that moved to the “random X” algorithm. Something that the Monero developers and community as a whole have been quite adamant about is there a version to ASIC mining rigs. While many other so-called ASIC resistant blockchains have given up the fight, the Monero devs have kept pushing back. Their view is that ASIC mining can lead to the centralization of the network. Centralization is a threat to any distributed network and especially one that relies on privacy. In order to stay off this threat the Monero developers have implemented a number of hard Forks that have rendered these ASIC-s mood. The random X upgrade will take this one step further by using random code execution and memory hard techniques. This is also great news for those of you who have GPU mining rigs as it means that ASIC-s won't be driving down the returns and increasing the mining difficulty. In fact random X has been optimized for CPU mining so this could further level the playing field to a wider array of participants. We can't talk about Monero mining without going through its native currency XMR. This coin was released without any ICO or pre mine or founders fund. It sits comfortably in the top 20 of CoinMarketCap rankings and has the highest market cap of any other privacy coin. It currently has a circulating supply of just over 17 million. Interestingly, there's no max supply. That's because the Monero economics works a bit differently. There will be a total supply of 18.4 million Monero. But unlike Bitcoin, which has a fixed supply of 21 million, Monero will continue to emit a 0.6 XMR per block infinitely. This is called “Taylor mission” and is scheduled to kick in in May of 2022. Why? Well, it provides an important economic incentive for the miners to keep mining. Miners will only mine as long as the ROI is there. Once block rewards drop to zero, and competition increases this ROI decreases. So the Monero developers have thought ahead for this. XMR like the rest of the crypto market has been on a wild ride. Monero is a completely open-source project with a wide array of developers working on it. That means despite what crypto journalism will have you believe, there is no founder or CEO of

the project. Yet there is a core team of developers working on Monero. One of the most well-known of these is Ricardo AKA “fluffy pony”. Ricardo is the lead maintainer on Monero and became involved with Bitcoin all the way back in 2011. As an open source project, Monero has to rely on donations from the public in order to fund new initiatives. This is done through their community crowd funding system or CCS. This mechanism gives the community the ability to either support the project through proposals or funding. There has been quite a lot going on in Monero repos over the past two years. On top of the forks that were done to stave off the ASIC-s there were a number of improvements and optimizations. For example there was the deployment of bulletproof on the Monero protocol. This greatly improved the efficiency of Monero transactions. Since this deployment the size of an average transaction has dropped by at least 80%. This also had a similar impact on the average Monero transaction fee. You also have the heavy development that is taking place on “KOVRI”. This is a C++ implementation of the “i2p network”. This will allow you to route your Monero related traffic through the encrypted i2p network, similarly to TOR. Why does this matter? Well, it will obfuscate your IP address and hide the fact that you are even running a Monero node on your PC. It's one more step to the holy grail of complete anonymity that Monero is striving towards. There are also a whole host of other improvements that we can look forward to on the Monero network. We just had the recent network upgrade and there are still a whole host of proposals being assessed. Monero is a pretty popular cryptocurrency. It does well over 100 million dollars a day in daily trading volume. It is also listed on quite a wide array of exchanges. These include many of the well-known platforms such as Binance, Kraken, BitRex and so on. It also does a whole host of volume on some lesser-known offshore ones. Wide exchange support is great for the price discovery of a cryptocurrency. It allows traders to get a better sense of the true price of an asset, undistorted by supply demand imbalances. How does the liquidity look for XMR? Well pretty good in general. Taking a look more specifically into some order books it is similarly impressive. From a market microstructure perspective Monero has got the liquidity and exchange support that allows easy conversion. While this is the case currently, it may face difficulty going forward. As we know Monero is private by default and has no way to opt out. This is a feature and not a flaw it does place exchanges in a sticky situation. Because they cannot track the transactions coming in, they have no way of knowing whether their

exchange is being used for any money laundering purposes. In order for a centralized exchange to effectively operate, they have to provide information to the regulators. The regulator's don't like Monero. We're left with a situation where exchanges either have to operate outside of particular jurisdictions, or delist Monero. We already we've seen exchanges such as OkEx and BitPay drop Monero. Could others follow suit? Can Monero still function with the resulting drop in liquidity? Or will decentralize exchanges be able to fill the void? All open questions that can be debated. Monero also has some of the most advanced cryptographic technology embedded in its protocol. It has the staying power and has proven itself through the years. It's fully open source with a community that's driven more by ideology than profit. They understand the importance of privacy and financial freedom. They're also aware of the challenges that the project faces and are willing to adapt to address them. This can be evidenced by their stance against ASIC miners and the work being done on KOVRI and other protocol updates. Exchange support could be a problem in the future. If the regulator's really want to, they can drive all Monero trading off of centralized exchanges. Yet Monero must be doing something right if it is viewed as such a threat by these regulators. Perhaps other avenues will be opened up to exchange Monero. Maybe we could see a time when it's just used like a normal currency. You won't have to convert your Monero. You can use it just like it was intended; untraceable peer-to-peer digital cash.

In terms of the price, Monero started trading around 25 cents a coin and it reached its all-time high close to 494 dollars per coin. This means that if you have invested at the time of its all time low and would sold off at its all-time high price you would have gained a 1976X. As an example, you could have potentially made $197,000 on $100 investment. To learn more about Monero, please visit the following website:

https://coinmarketcap.com/currencies/Monero/

Here you find additional links to Monero's website, Explorers, Source Code, technical documentation, historical data, on-chain Analysis and charts for market capitalization and price.

Chapter 20 Verge

The disadvantages of Bitcoin are its privacy. It's possible to discover the details of the transaction including the standard personal information with a little technical investigation. To answer this security concern numerous coins have been developed that focus on offering privacy to users. Verge is one of this privacy coins. It has the same purpose as Bitcoin but the way it distinguishes itself is by offering stronger privacy then Bitcoin. Bitcoin is not anonymous and Verge is striving for complete anonymity. Its intention is to be used for global transactions. The company hopes that it's low transaction cost and high transaction speeds will attract users into buying and spending the coin. Verge integrates TOR into the blockchain which gives additional security. Verge also wants to implement smart contracts in the future. Verge is a community driven project. It is entirely open sourced and the community has great influence on the decisions that are made. There are no pre-mined coins or ICO which means that the direction Verge takes will by solely decided by regular users.

Most cryptocurrencies have their own algorithms to verifying degrees and ensure privacy. The question is what makes Verge so different from other privacy coins. Well, Verge have it’s own district way to strengthen privacy. Verge will have the utility that is the first among privacy based coins. This will help Verge to have a better chance of winning over the market. Verge was launched in 2014 and was first named “Dotcoin dark”. Dotcoin dark then rebranded itself to Verge in 2016. The mission of the team is to bring cryptocurrency to daily transactions, given both individuals and businesses flexible payment options. The raft protocol is the key to this flexibility, allowing users to choose between private and public Ledger's. Verge is completely community driven. No ICO was organized nor any pre mind coins and it was built on the Bitcoin blockchain network.

How does Verge works? Well, Verge ensures privacy by hiding the users IP addresses with TOR and ITP integration. In case you don't know what TOR and ITP are, in a nutshell these protocols allow you to remain anonymous on the internet by directing your traffic to a hidden network. This makes it difficult for anyone to monitor or locate your traffic.

ITP offers all of the same benefits as TOR with one additional advantage. It

is a network within the internet. ITP ensures that any information is fast around the network, data also will stay within the same network and be inaccessible to any outside interference. ITP tunnelling features provide an additional layer of security. A simple VPN would only protect your privacy so long as you ISP doesn't reveal information. But the use of TOR and ITP ensures that your data has complete protection by integrating these networks with Verge. Therefore the transaction conducted become untraceable.

Verge offers five different proof-of-work algorithms for mining. Providing a choice of five different algorithms encourages inclusion as a wider variety of users will have the chance to mine and influence the network. Therefore if the algorithm require greater mining resources, users can simply switch to another algorithm.

The team has stated they want to provide equal access to mining and this is the reason behind the implementation of five algorithms,

They are the benefits of having better security and the lower probability of a 51% attack. Verge also wants to make the network as well the coins as accessible and user-friendly as possible. Therefore for this reason they have released supporting wallets on various platforms with a particular focus of the mobile space.

They have announced that they intend the coin to be used for everyday purposes and would support as many wallets as possible. The preferred wallets are selected by the team it's called Electrum because it has native support for TOR or ITP. Electrum is a well-respected hot wallet that is fast and user friendly and not source intensive. Users can also store the coin on cold storage so the adoption is also good.

Electrum also requires multi signature support. It works like this. You've got an Electrum wallet on both desktop and mobile. In order to conduct a transaction, a signature will have to be verified from both devices before it takes place. This way theft is less likely to occur because both devices would have to be compromised.

Verge actually has two mobile wallets. One separates on TOR and the other on ITP. Both of these wallets operate like Electrum and the data user does not need to download the entire blockchain. Through the simple payment verification technique, the transaction that passes in a particular block can be verified. The SPV technique allows for rapid transactions because much less

block information is downloaded. The Verge wallet will also support paper wallet QR code.

The Wraith protocol is the most compelling feature of Verge. The Wraith protocol allows users to select between a public and private ledger. When the Wraith protocol isn't used, the private Ledger is used and transactions are not visible on the blockchain. When it's turned off, the public ledger is used and visible on the blockchain.

This is a good solution to the demand for some transparency in cryptocurrency when a store or merchant wishes to record transaction for accounting purposes, the public ledger will come in handy. Verge gives users the options to transact privately or publicly. They also have another protocol called Stealth Addressing. In a nutshell, a one-time public key is generated that is visible to the blockchain but the sender and recipient are the only ones aware that they are involved parties. The recipient will have a one-time private key that correspondence with this one-time public key which will allow him or her to access the funds.

This prevents the recipient from having his addresses publicly linked to a transaction. Stealth addressing is not a new technology as Monero and Bred coin uses this method too. Verge seems to be hoping that in combination with hidden IP addresses it will be the most trouble solution to the privacy problem in the cryptocurrency space.

To protect the sender Verge is looking into method called ring signatures. They also use another protocol called Rootstock.

The idea seems to be to challenge the Ethereum smart concert platform by providing easy to use mechanisms the users. Verge token will be received on the RSK chain which can then be used on the RSK network for spending it. Another outstanding point is that RSK achieves 400 transactions per second. Currently Verge transacts at a rate of about 100 transactions per second. The implementation of RSK would be great progress. The RSK development team has a goal of achieving 2,000 transactions per second. If that succeeds, it would make Verge one of the best tokens to use for global transactions. Why is the Verge token needed? Well, users want to have several more coins offering better privacy features and Verger is claiming to be completely anonymous. However there is resistance to fully autonomous coins as well. The issues is that a system without untraceable transaction will be a breeding

ground for criminal activity. This is one of the main arguments that governments move forward for the regulation of cryptocurrency. Nonetheless, privacy is a fundamental right for every person. The problem is that a lack of privacy intersections is more dangerous than the possible rise in criminal activity. If a connection is made to your personal data on a single transaction on the blockchain, your entire transaction history is exposed. Furthermore, if a business conducts a transaction in cryptocurrency, a competitor can see the payments arriving and leaving the account and that information that could compromise the business.

Verge will allow a business to keep its transaction and maintain an advantage. The team dives into the technical details of privacy implementation in the black paper.

The main team comprises of 13 people with experience in various fields. The team is lead by a core developer and the founder of Verge. His expertise lies in network security and blogging with 20 years of experience.

The prominent members of the team include Sascha, the Vice President of operations and Kieran Daniels the President of Marketing. Overall the team is quite experienced and well-respected.

Verge main competitors are Monero, Dash and Zcash however there is a lot on their roadmap and many are concerned that the development is not proceeding at pace they wanted to. But they have been keeping the community updated which is always great.

Purchasing the Verge token is simple but you can't buy directly so you'll need the buy first Bitcoin or Ethereum and then purchase Verge with those.

Verge is in a lucrative niche and the privacy race is still just beginning and there is no indication which coin is going to win. Verge community oriented approach is a positive sign but it must be backed up by consistent progress. Its anonymity is also not perfect. Like every other privacy coin there are differences perhaps RSK implementation will give it an edge over other coins in the future but time will tell. The development team is solid with multiple years of experience but privacy coins creation and maintenance is not an easy job.

In terms of the price, Verge started trading around $0.000079 a coin and it reached its all-time high close to $0.24 per coin. This means that if you have

invested at the time of its all-time low and would sold off at its all-time high price you would have gained a 3157X. As an example, you could have potentially made $315,789 on $100 investment. To learn more about Verge, please visit the following website:

https://coinmarketcap.com/currencies/verge/

Here you find additional links to Verge's website, Explorers, Source Code, technical documentation, historical data, on-chain Analysis and charts for market capitalization and price.

Chapter 21 Beam

Beam is a privacy oriented open source cryptocurrency that focuses on scalability, using the Mimblewimble protocol. Using the Mimblewimble protocol, Beam is creating a method that significantly reduces the amount of bloat which resides on the blockchain. Doing so provides much greater scalability for future iterations. The beam project wants to create a new privacy enhanced user friendly cryptocurrency that offers transparency and decentralization. However to get a better understanding of beam you need to have a good grasp of the Mimblewimble protocol and how it works. In 2016 an anonymous user by the name of Tom Elvis Jedusor proposed a protocol he referred to as Mimblewimble. The Mimblewimble protocol integrates several concepts into one hybrid blockchain. This creates a network that offers improved privacy and efficiency. As a result the two areas addressed by the Mimblewimble protocol are scalability and privacy. Thanks to the privacy inherent within the Mimblewimble protocol, Beam offers strong fungibility. If you aren't familiar with the term fungibility, is a currency property that does not distinguish between units of value. They are all considered equal. With Mimblewimble, the person receiving the transaction can generate a blinding factor. What does that mean? Well, it means verification on the Mimblewimble protocol always requires that the number of inputs and the number of transaction outputs always result in 0. Only those participating in the transaction can view the data it contains. This includes the addresses and the value of the transaction. One of the biggest benefits of using the Mimblewimble protocol and Beam is that it offers the same privacy and security as well-known coins like Monero and Zcash and it does so without sacrificing efficiency and transaction speed. For performance and scalability, Mimblewimble removes unnecessary transactions while simultaneously combining intermediary transactions which helps to improve efficiency on the network. When transactions occur within a block on the Mimblewimble protocol they look like a random mixture of outputs and inputs as opposed to showing a corresponding list of the same information. Due to this type of behaviour the Mimblewimble protocol lends itself to being significantly more scalable than other blockchain projects. Users can sync to the network easily and quickly which provides a more practical use of network nodes. However the question remains. Can Beam really offer quick and efficient scalability to

blockchain platforms? Using the Mimblewimble protocol means Beam has access to the cut-through features which are what makes scalability a reality with the project. Here's how it works. First the protocol allows for transactions to merge by cutting through the intermediate transactions. Intermediary outputs that form a block are presented as one transaction which allows the system to track the current state without having to do the same for all transactions. When a new node initially joins the network, it begins working with an already compressed history. For example it might be using a history that only contains blockchain headers and system state information. Since the new node doesn't need to retrieve the entire history of the blockchain, this approach significantly reduces the amount of information needed for a node to begin verifying or mining new blocks. Before we transition to the tokens of Beam, let's talk about the Mimblewimble protocol and more about the project as a whole. For starters the project states that the Beam network is for use as a store of value rather than payments on a day-to-day basis. The network can perform 17 transactions each second which is much faster than Bitcoin and other more notable privacy crypto currencies. Yet this amount is not yet high enough to use Beam as a payment method. Beam understands this which is why they're looking at possible future alternatives through a second layer solution. One last area I want to address that often gets overlooked with the beam project is its auditability feature. This feature gives both individuals and business the ability to provide financial history to auditors in a provable and secure way. By generating multiple key pairs and a public key created by the auditor, companies can accept crypto as a store of value without disclosing transactions or funds to anyone else. Keep in mind that auditability is completely optional. Users do not have to allow this functionality when using Beam.

Beam is a privacy coin by default. It allows no open transactions. So even if someone is reading the blockchain, they're not going to gather any valuable information. Users on the beam network have complete control over their own privacy. This means that you decide what information you want to share and who you want to share it with. Let’s now talk about the Beam coin. The Beam project held no ICO and did not offer any pre-mined coins. Something that many cryptocurrency projects don't often do. On the other hand Beam was significantly rewarding early investors. Beam has a supply of nearly two hundred and sixty three million tokens which the project uses on a deflationary emission schedule. This is based on block rewards during having

events along the same lines as Bitcoin. For those who enjoy mining, Beam ensures that decentralization occurs on its network by becoming ASIC resistant for the first 18 months. This means that GPUs can mine Beam. Who is the team behind the Beam project? Well, the Beam project team brings plenty of experience and background in the entrepreneurship and technology industry. For starters, the CEO Alexander's Idol has began his career working in software development. Alex Romanov is been CTO and comes from a background involving several complex projects, while managing large R&D teams. He's been at the help of the R&D and since Beam’s inception. It's safe to say that Beam has an excellent leadership team but since the project is still new, it's tough to determine how well the team has met its targets. Still they continue to provide regular updates which is a positive sign for any cryptocurrency project.

You can also take a look into their github repos and monitor the extent of code commits. You can find there are a lot of codes have been committed.

Beam has released Multi-sig capabilities, support for Trezor and Ledger hardware wallets and the creation of a decentralized marketplace in the Beam wallet, which allows for atomic swaps.

The Beam coin is available on many different exchanges like Hotbit, BW.com, Dragon EX and Coinsuper. The coin was recently listed on Binance if you prefer to stick with a well-known exchange, you can purchase Beam there too.

You can trade Beam against Bitcoin, Etherium and USD T on most of these exchanges. Once you have your coins you can keep them in a wallet for safekeeping. Beam has its own wallet available right on its website and it's available on Mac OS, Linux, Windows Android and iOS.

So no matter which platform you prefer and if you're looking to store your Beam in a hardware wallet, Beam is already released for Trezor and Ledger integration too.

As one of the first Mimblewimble cryptocurrencies, this project has been pretty excited, especially when you think about the potential that comes from a truly scalable privacy blockchain. You also have a pretty strong team behind the project that has been constantly pushing updates to the protocol which is always a good sign. Having said that, the main challenge here is that they're already privacy coins heavily entrenched in the cryptocurrency

market. Beam is fighting an uphill battle against coins like Zcash and Monero, so it's going to take quite an effort for it to succeed. Beam could become a great example of how well the Mimblewimble protocol works, but is much too early in the project to make a serious determination. Yet if Beam can successfully navigate these challenges and continually deliver on its development goals, there is strong potential.

In terms of the price, Beam started trading around 68 cents a coin and it reached its all-time high close to 2.42 dollars per coin. This means that if you have invested at the time of its all time low and would sold off at its all-time high price you would have gained a 3.5X. As an example, you could have potentially made $350 on $100 investment. To learn more about Beam, please visit the following website:

https://coinmarketcap.com/currencies/beam/

Here you find additional links to Beam’s website, Explorers, Source Code, technical documentation, historical data, on-chain Analysis and charts for market capitalization and price.

Chapter 22 Grin

Grin is a relatively new privacy coin that was built on the Mimblewimble protocol. Mimblewimble was a proposal developed to increase bitcoin's privacy, scalability and fungibility. The exact mechanics of how the Mimblewimble protocol works can be hard to wrap one's head around, but it basically eliminates bitcoins UTXO model. This is then replaced with a multi signature for all inputs and outputs. These are confidential transactions that use a Peterson commitment scheme where the parties will share a blinding factor. This blinding factor encrypts the inputs and outputs of the transactions along with both parties public and private keys. Given that Grin uses the Mimblewimble protocol, there are no identifiable or reusable addresses. All transactions appear as random data to outside participants. Just like Monero and Zcoin, it has a privacy by default. All Grin are fungible, but the privacy aspect is only one component of Mimblewimble. It is also has a lot more efficient transaction mechanism which means it can scale more easily. In fact grin is able to scale mostly with the number of users and minimally with the number of transactions. This results in a large space saving compared to other blockchains. Apart from the obvious privacy and scaling potential that Mimblewimble affords Grin, there are a number of reasons why Grin itself is a project that is interesting. Most importantly it is a completely open-source blockchain that was started with no pre-mine or ICO. Also there's no founders reward at all. Unlike some other privacy coins that reward founders with the percentage of block rewards, Grin has none of that. Grin is also not controlled by any company or individual and is funded entirely by community donations. All of the spending from these development funds are displayed in a transparent manner. So far they've been able to raise about 190 bitcoins. Compare this to some of the projects that did ICO-s is back in 2017, many that raised north of 30 million dollars, have either developed nothing or evaporated entirely. When it comes to mining Grin, it also uses a pretty unique proof-of-work algorithm called the "CooCoo cycle". This is a memory bound algorithm and it was developed to be ASIC resistant. Another win from minor decentralization. Something else that you'll notice aback Grin is that they have a steady emission of one Grin per second.

Some people concern as it meant a steady rate of inflation with no capped supply. Well, a steady rate of inflation and pride appreciation are not

mutually exclusive. All that matters is the rate of said emission compared to broader demand. Monero will also have what is called “Tail Emission” which will kick in in 2022. Grid sounds great, but are there any challenges that it faces? Well, firstly I would have to say it doesn’t have enough exchange support. Whereas Monero and Zcoin are both listed on some reputable exchanges, I can't really say the same for Grin. The only exchanges I would really consider are Bittrex or maybe KuCoin. Even if it did have more exchange support, its privacy by default could face the same challenges as Monero and Zcoin. But perhaps the biggest challenge for Grin is that there is a vulnerability that was discovered in the Mimblewimble protocol.

Not a vulnerability that puts users funds at risk, but one that allows an attacker to de-anonymize transactions. The privacy vulnerability also only applies to senders and receivers and not to the actual amounts being transacted. Nevertheless, this is an issue for Mimblewimble based coins but then Grin is a new project and the developers were aware of this potential attack vector. So as they continue work on the protocol, I remain cautiously optimistic.

In terms of the price, Grin started trading around $2.40 a coin and it reached its all-time high close to 13.11 dollars per coin. This means that if you have invested at the time of its all time low and would sold off at its all-time high price you would have gained a 5.4X. As an example, you could have potentially made $540 on $100 investment. To learn more about Grin, please visit the following website:

https://coinmarketcap.com/currencies/grin/

Here you find additional links to Grin’s website, Explorers, Source Code, technical documentation, historical data, on-chain Analysis and charts for market capitalization and price.

Chapter 23 Particl

Particl pronounced as “Particle” has an ambitious goal of building a decentralized economy supported by all the key elements of blockchain technology; privacy, interoperability and security. There are three key features that are part of the Particl ecosystem. These are the Particl platform the Part coin and the open marketplace. Let's take a closer look into each one of these. The Particl platform is where decentralized application or DAP developers can build their own privacy centric daps. Many different kinds of daps can be developed on Particl but the common thread that links them all together is their use of the Part coin to process transactions. The Part coin is the utility token which powers the platform. It is a privacy coin that can send anonymous transactions as well as be used for voting in the ecosystem. It can also be staked for an additional source of income. Finally the open marketplace is actually the first dap that was built on the platform. It's a completely decentralized and private marketplace where people can buy and sell anything they like. Part coins are used as the medium of exchange and these features solve many of the biggest problems with e-commerce platforms today. Lack of privacy, data breach caused by poor security, lack of censorship resistance and high transaction fees. Something else that I found quite interesting about Particl was their proposal mechanism. This is basically a way for those in the community to submit the proposal that can then be voted on. This includes an aspect of decentralized government to the protocol. The Particl team is quite extensive and they come from many different backgrounds. There are software engineers, entrepreneurs and a host of well-known strategic advisors. Particl is also quite unique in that they did not hold an ICO and did not conduct any pre-mines. This means that the project is more decentralized and hence fairer. Currently Part is available on 4 different exchanges although the bulk of the trading is taking place on BITTREX with over 80% of the volume. This volume is quite thin currently which could impact liquidity for large orders. If you want to store Particl then you can either use their proprietary wallet or you can store it in a Trezor. Something else that is pretty neat is that you can stake your coins from a hardware wallet. This is called cold staking your coins and keeps them safe while still earning that staking return. In conclusion, Particl is an interesting project that's more decentralized than most. Their unique approach to privacy

centric daps and the open marketplace is quite unique amongst crypto projects. They will need to increase the trading volumes across more exchanges if they're to increase adoption and awareness of the project.

In terms of the price, Particl started trading around $5.29 a coin and it reached its all-time high close to $43,36 per coin. This means that if you have invested at the time of its all time low and would sold off at its all-time high price you would have gained a 8.2X. As an example, you could have potentially made $820 on $100 investment. To learn more about Particl, please visit the following website:

https://coinmarketcap.com/currencies/particl/

Here you find additional links to Particl’s website, Explorers, Source Code, technical documentation, historical data, on-chain Analysis and charts for market capitalization and price.

Chapter 24 Horizon / ZenCash

There are a lot of privacy coins currently on the market, all offering unique and supposedly revolutionary technology. Horizen's ZED is one of those. This is a fork of a cryptocurrency used to be called ZenCash until a rebranding in 2018. But this was much more than a rebranding. The Horizen team used it as an opportunity to reinvent the cryptocurrency with a whole host of features and improvements. Yet is it a privacy coin really worth considering? Horizen is a privacy focused blockchain that is a fork of ZED classic which was itself a fork of Zcash. As such it is one of the privacy coins that makes use of Zcash as ZKsnark technology. This highly advanced privacy technology makes use of zero knowledge proof. The Horizen network has been created to encompass a variety of privacy focused projects which include a decentralized autonomous organization, a private messenger Zen chat, an anonymous publishing platform Zen Park and a domain fronting service called Zen Hide. In addition there is the Zen cryptocurrency, a full suite application called sphere by Horisen Zen nodes and Horizen's blockchain. While many people feel that security and privacy are topics that only pertain to criminals, conspiracy theorists and the paranoid, the fact is in today's world cyber security should be a major concern for everyone. Cyber security experts at Norton estimate roughly 60 million Americans have had some impact on their lives and data due to identity theft, and that by 2023 half of all the data breaches in the world this figure will double. Furthermore, it's important for people to understand that it's not your personal computer you need to worry about when it comes to hackers. The majority of hacking is at a far greater scale, and impacts tens of thousands of people at a time and in some cases up to millions. We all have accounts with entities and we trust with our data such as Google, Microsoft, Visa and even your National Government. These are the places where hackers strike and you can bet that these companies and governments follows stringent security measures to protect the data they hold. There are even laws in place to ensure that's the case, although it seems the penalties for allowing a data breach aren't enough to encourage complete security because data breaches are still common enough. Horizen focuses on adding privacy for enterprise applications. That includes messaging and publishing as well as private and secure data storage on the Horizen blockchain. The Horizen or ZenCash at the time did not hold

an ICO but since then was created as a fork of the Zed classic blockchain. That fork occurred on May 23rd 2017 at block number 110,000, and Zen was issued on a one-to-one basis to holders of Zed CL. Then on the 22nd of August in 2018, the ZenCash team decided that a rebranding was in order. This was done in order to provide a springboard for much more than just a privacy coin. Zen uses the Equihash algorithm to achieve consensus and is a proof-of-work blockchain. The current block reward for Zen is 7.5 Zen with blocks being mined roughly every two and a half minutes. Just like Bitcoin the rewards are half roughly every four years. Unlike Bitcoin, the block rewards are not all for the miners. Instead, 70% goes to the miners, 20% is split evenly between secure nodes and super nodes and the remaining 10% goes to the Horizen team treasury. Secure nodes or what you might normally consider to be master nodes. They require the node owner to stake 42 Zen. The Horizen nodes are unique in that they use node to know TLS encryption to secure all communications. There have been some criticisms regarding the Horizen project. These include the encrypted key generation event known as a trusted setup which could allow a bad actor to create unlimited send coins if they were to compromise the process. There are also rumors that the original code used to create Zcash may have had a police backdoor included, and this backdoor has also made it to the Horizen implementation of the code although there is no proof of such a backdoor for either Horizen or Zcash. With its long history stretching back to Zencash, it shouldn't be too surprising that Horizen has a solid and diverse community behind it. Over a Twitter, there are over 46,000 followers and the Facebook page has over 8400 followers. The sub-reddit for the project is just shy of 3000 readers which isn't the biggest read at following but it is a strong one with regular updates being posted and multiple comments on each posting. Telegram was a bit more discouraging with just under 1,700 members. As mentioned earlier there was no ICO for Zen since it was created as a fork from Zen classic. There is a total supply of 21 million Zen just like Bitcoin and the circulating supply is just over 8.5 million coins. Zen is was held up pretty well during the 2018 bear market. The price bottomed out in mid 2019 and has been trending higher since October 2019. The all-time high was $67,7 on January 10th 2018, and the all-time low was $3.09 set on July 31st 2017 which was just two months after Zen started trading. The coin did come very close to that all-time low recently however touching $3.14 in September 2019. Although Horizen has rebranded and laid out its renewed vision one has to ask whether

this has been translated into actual development output. One of the best ways to determine this is through their open source code bases. Given that Horizen is open source, we can dive into the Github to get a sense of how much code is being pushed. Horizen has made itself stand out from the crowd of privacy coins by getting away from the focus on basic anonymity and privacy. The full suite of tools being offered by Horizen not only to individuals but also to enterprise users and that could be the key to Zen adoption. The main criticism of Zen is that it uses the same zero cash protocol that was developed for Zcash and there are rumors of a backdoor in the code that would basically eliminate any privacy for the coin and blockchain. But Horizen has a lot going for it from the Zen chat applications to the development of Siddha chains that will allow for the hosting of any dap or blockchain right alongside Zen. With these pieces in place and with the coming launch of Zen DAE Horizen has positioned itself well to become a sustainable blockchain ecosystem. the tools being developed are suited to the enterprise user. This is because horizon understands that enterprise users tend to remain loyal to a technology once it's adopted an enterprise users often have the ability to pay well for long periods of time. The piece needed now is the delivery of an SDK which will allow for the rapid spread of Zen on the Horizen network.

To learn more about Horizen, please visit the following website:

https://coinmarketcap.com/currencies/horizen/

Here you find additional links to Horizen’s website, Explorers, Source Code, technical documentation, historical data, on-chain Analysis and charts for market capitalization and price.

Chapter 25 Overview of Privacy Coins

In this Chapter, I am going to give you an overview of all the privacy coins that I have mentioned so far. If you made it to this Chapter, you know that I have introduced different kinds of cryptocurrencies which are revolving around privacy functions so you might be confused and want to find out which one is or which ones are safe to invest. First and foremost, I am not a financial advisor, therefore don't take my word as a financial advise. In case you seek a financial advise, you should hire a professional because this book is for education purposes only. This book has a collection of a large number of privacy based cryptocurrencies so you have them all in one place but it doesn't mean that I recommend them all for you to invest. I have spent some time on researching on the history of each coin and calculated what kind of ROI or return on investment could have been done. You can use this information as a tool for your own decision before making any investing. However do not rely only on my own figures, instead do your own research and be confident about any investment you make. This is one of the most important fundamentals of the cryptocurrencies that they are optional and no one forces you to have a specific currency. For example if you live in the UK, most of the shops are only accepting British Pounds only. So if you have Euro or dollars in UK and going to the shop, nobody will accept it as a payment method. If you are staying at a Hotel, they should have an exchange service but if you work in the UK, you will get paid in British Pounds. Same thing applies if you work in Germany; you will get paid in Euros. But if you want to invest part of your portfolio into cryptocurrencies, it is completely up to you and that's your own choice. Which privacy based coin is the safest to invest? Well, the answer is something that you might don't like. The fact is that there is no safe crypto asset out there. There are no guaranties. If any cryptocurrency you come across that provides guarantied daily, weekly or monthly profit that's most probably a scam. You must not forget what happened with Bitconnect and those have lost their entire life savings. It doesn't matter how good the return sounds, please try to avoid scammers. You should always be sceptical no matter what cryptocurrency is in question. You should always try to look at the history of the coin. For example,

- How was it launched?
- Who raised money for it?

- What platform was it built on it?
- What's the purpose of the project?
- What kind of advancements they have created since their inception?
- How many exchanges are dealing with it?
- If you invest now but you change your mind, can you sell it?
- How long is the crypto asset on the market since?

For example 1 year might be not enough to prove that is not a scam, like Bitconnect was. Bitconnect was out for more then a year and most people have not touched it whatsoever. But then suddenly few people were promoting it, and for some reason people forgot what scam means. Also if the project is only a month old and seems like the price and market capitalization is growing dramatically, don't forget that it might be a pump and dump. I told you that some pump happens in a day, some going on for weeks, but professional pump and dumpers know how to manipulate the market. They might be happy to pump the market for long a month or even months like Bitconnect did. But in the other hand like in the case of Bitcoin, it was fairly mined at the beginning. There was no ICO or fundraising for the project as the Cypherpunks have volunteered to contribute to build it for no money in return. The value of Bitcoin at the beginning was nothing and only over time people found value in it. Bitcoin didn't become an overnight success, and then disappeared like hundreds of other scam coins. If there is a crypto asset that I truly recommend is Bitcoin for the purposes just mentioned amongst others. In the world of crypto there is no guaranty and if someone says that he is either lying or doesn't know what he is talking about.

Chapter 26 Privacy Coins No1 Privacy Based Coin

How much money you have, what you spend it on and who you send it to? There are many people who would love to know this information. This is precisely why privacy coins like Monero are coming into their own. In this chapter I'm going to share with you exactly why I am bullish on Monero from the tech updates to industry shifts and regulatory action. I'll also be looking at its compelling economics and explain why I think Monero has so much value. Much like Bitcoin, Monero is a peer-to-peer electronic cash, but it was designed specifically for privacy as its blockchain is completely hidden. This therefore means that the XMR cryptocurrency is completely fungible meaning that each unit of Monero is completely indistinguishable from the other. Much like the one dollar note that you have in your pocket is the same one dollar note that your friend has in his. While you may think cryptocurrency is fungible it's actually not the case. Those that can be tracked such as Bitcoin or Ethereum have a transaction history which could make them less valuable. They could be linked to a hack or to the dark web. This would make them incredibly hard to offload. This is all because the blockchains are transparent. Transparency is essential for the trust in a decentralized network. So it's hard to square the circle between a private, hidden and fungible cryptocurrency with open source decentralized blockchains. But Monero is able to do this with some bleeding edge advances in cryptography. For example through the use of stealth addresses users are able to keep their unique Monero address while receiving inward transactions with a one-time public address. The exact mechanics of this is way beyond the scope of this book but it basically means that you can easily send an address to someone so that they can send a payment. Still no one else will be able to see that the end recipient of the payment is you, thanks to the use of these stealth addresses. Something else that makes Monero tick is the use of ring signatures. This is a mechanism where each transaction can be signed by a collection of other possible signers. When you include this ring of possible other signers, you're making it impossible for anyone to pinpoint exactly who signed a transaction. If that was not complicated enough you also have ring confidential transactions or "Ring CT". This is the feature that allows you to hide the transaction amount. All this is just the tip of the iceberg when it comes to the tech behind Monero. The main thing to take away from this is

that transactions on Monero are completely anonymous. You may have a public address but there is nothing that anyone can glean from it. Not how much has been spent or received or where money was sent or received from. A black box of privacy magic. This privacy comes with a cost. It means that Monero has made some powerful enemies. It was only inevitable that regulators were going to start taking notice of Monero. Indeed they were initially incredibly sceptical of Bitcoin and other cryptocurrencies back in the day. The old money laundering and drug dealer monikers were used. This was until they were able to get a full grasp of the Bitcoin blockchain. Thanks to its transparent nature and some incredibly powerful blockchain auditing tools, they were able to fully track Bitcoin transactions. They use these tools with great effect and have racked up case after case that was solved through some simple blockchain audits. Agencies like the IRS, FBI and DEA are much less worried about the risks of Bitcoin. Monero on the other hand is a whole other kettle of coins. It's clearly a major concern for these guys and actions by these agencies are further proof of this. For example, recently the Department of Justice released a document entitled “Cryptocurrency Enforcement Framework”. If you want to get your own copy, please visit the following webpage:

https://www.justice.gov/ag/page/file/1326061/download

This is basically an overview of the DoJ's thinking on cryptocurrency and its potential for illicit use. This was over 80 pages long and there was a lot of irrelevant information in it. One of the most glaring facts about it is that they clearly have their eyes on privacy coins. In fact they went as far as to say that the mere use of privacy coins is “indicative of possible criminal conduct”. So the mere use of these privacy coins rings alarm bells over at the DoJ. There is no point to get into how hypocritical this is given that the majority of crime is carried out with US dollars but it does show the level of scrutiny privacy coins are getting. Indeed over at the IRS they're also keen to get a peek of what is going down on the Monero blockchain. This is one of the reasons that they recently released a 625,000 dollar bounty on any firm that could crack Monero. They subsequently awarded the contract to Chainalysis and Integra FEC. The hope of the IRS was that these two agencies could develop tools that could be used to track Monero transactions. It's not just the US regulators that have their sites on Monero. There are numerous other global agencies that would love to have the ability to put a finger on Monero transactions.

Those include EC3 European Cybercrime Centre, NCA or National Crime Agency and Europol. These agencies pose an existential threat to Monero. Or Monero poses an existential threat to their control. They've been at this for quite some time. The mere fact that the IRS is looking for outside help to crack it, is an indication of how desperate they have become. Surely if the IRS, DEA or FBI is unable to crack Monero with the resources of the US Government behind them, two blockchain auditing start-ups probably won't be able to either. Moreover, there's probably a lot more money to be made by actually cracking Monero than a mere 650,000 dollars. If a really determined adversary could crack it, the payout would be worth a lot more than that. Monero must be doing something right if there's such a threat to these guys. But there is one potential action that these guys could take that will make it hard to use Monero. This is enforcement action on any of the crypto exchanges that allow trading of it. That DoJ document has made it pretty clear that “any exchange that chooses to list anonymity enhanced cryptocurrencies will have to make sure that they can implement the correct AML/CFT procedures on the coins coming onto the exchange.” This cannot really be done. Unlike other privacy coins such as Zcash for example, Monero's privacy is not opt-in. It's all or nothing privacy which is great for the broader network but not great when it comes to exchange listings. Indeed it's well known that many large crypto exchanges have bulked at the opportunity to list Monera as they know of the potential regulatory risks. There are a few exchanges that have delisted Monero because of this. Some may think that this is a cause for concern. Well, yes it is. If there's no liquidity for trading Monero then it cannot really be used as a currency. But the Monero developers are not the ones to take that risk lying down. There is already a lot of work that's been done on XMR-Bitcoin cross-chain atomic swaps. These would allow users to swap Bitcoin and Monero on chain without the need for any centralized authority. Users could build an open source DEX that would allow them to trade between the two currencies. Once Monero has been converted into Bitcoin, that would solved a lot of the problems that come from the lack of liquidity. A Monero developer called Joe has raised over 2000 XMR in order to continue his work on these swaps. More recently, a team from commit network presented a proof of condition for Monero-Bitcoin atomic swaps. It's worth pointing out that developing these swaps is anything but simple. There are a number of unique differences between Monero and Bitcoin that make it much harder to conduct these

swaps compared to say Bitcoin-Litecoin for example. But having said that developing a privacy coin as complicated as Monero was thought impossible a few years ago. So don't underestimate the resolve of an ideologically driven collection of hardcore cypherpunks. The exchange threat is not too much of a concern to be honest in any event. The mere fact that we have to rely on these centralized exchange services as the gatekeepers to our crypto trading is alarming. Now addressed two of the most pressing concerns for Monero and why I don't think they should really be concerns. But there are a number of other factors that could make you a fan so let's take a look at some of those.

There are a number of threats that face any cryptocurrency network and one of the most well-known is that of centralization. This is after all the antithesis of a decentralized blockchain. This is particularly true when it comes to minor centralization. For example there is over 65% of the hashing power for Bitcoin comes from Chinese mining farms. This is no doubt a pressing concern that bitcoiners have been worrying about for the longest time. This centralization comes down to the nature of Bitcoin's consensus method. Through the use of specialized mining equipment called ASIC-s, large mining farms have a competitive edge over your smaller miners. These ASIC mining rigs have also been developed for a number of other proof-of-work blockchains and have had similar effects. Litecoin, Zcash, Dash and the list goes on. In fact over the past three years the Monero community was concerned that a kryptonite Monero's previous algorithm ASIC had been developed. They were worried that it was being used to secretly mine XMR by the manufacturers. So the developers did what they could to neutralize the threat. They went through a number of hard forks designed to tweak the algorithm and render them ineffective. This worked for a while but eventually they decided a more permanent solution was in order. Therefore in November 2019 they decided to hardfork the Monero blockchain and implement a new proof-of-work consensus called “Random X”. This is optimized for CPU mining. This means that anyone with a CPU can mine it whereas previously you would have needed expensive GPU-s and even pricier ASIC machines. This means that Monero has become much more decentralized. It means that no longer is hashing power concentrated in the hands of a limited group of miners. Moreover if you look at the Monero hash power chart, you can see that it's increased substantially since the fork. To view the chart, please visit the following site:

https://bitinfocharts.com/comparison/monero-hashrate.html

The kryptonite and random x hash are not exactly equivalent but it is the trajectory here that interesting. Apart from the fact that the random x upgrade has made it more secure, it also shows that the Monero community is dedicated to keeping up the fight against centralization in any form. This is just the network security aspect. Two years ago Monero implemented “bulletproofs” which dramatically reduced the size of transactions. The end result was much cheaper transaction fees and much faster transactions. Win-win for usability. The network keeps evolving. In October 2020, Monero had another hardfork to implement a new compact ring signature scheme in version 13. Moving on to XMR tokenomics and price potential, if you've been paying attention to the price of XMR, you'll have seen it slowly gaining ground and moving up the CoinMarketCap rankings. Could wales be increasing their Monero position in anticipation of further moves to the upside? Well you might try to pull up the largest Monero addresses to get a sense but you will see nothing because we're not supposed to. So we cannot really know who is stacking Monero. But what we do know is that positive volume and technical sentiment has been pushing it up over the past few months. In fact XMR is at levels that have not been seen since 2018. What's interesting about Monero is its tokenomics, or more specifically its emission schedule. Much like Bitcoin, Monero has decreasing block rewards. But once Monero reaches its total supply of 18.4 million in May of 2022, there will be what is termed “tail emission”. This is a constant block reward of 0.6 XMR that will be paid out infinitely. This means that Manero's total supply is not capped. There will be a constant 0.6 XMR added to the supply after every block. Compare that to Bitcoin where there will only ever be 21 million Bitcoin and that is the cap. As we approach that supply limit Bitcoin block rewards will approach zero as will the inflation. So some will say I would rather pick the coin with a fixed supply. It's limited and will be a scarce asset. Well, that is true but there are long-term security concerns for Bitcoin in a world with zero block rewards. Miners are no longer being rewarded for pushing blocks through. They have to rely on transaction fees in order to remunerate their work. The two scenarios here is that either the miners stop mining which brings the chain to a complete hold, or they do mine but sending transactions becomes prohibitively expensive. Neither of these is beneficial for the long-term health of Bitcoin. Not trying to make a bear case for Bitcoin and layer 2 solutions will present a viable alternative for sure

however, it does show how forward thinking the Monero devs were to include that “tailor mission”. We can now be guaranteed of constant block rewards for the miners post 2022. One that will incentivise them to keep on mining and securing the network. You should also note that although this is a constant block reward, the inflation rate itself is also decreasing. So unlike many other coins that have aggressive staking returns that devalue the total value of the network, Monero will preserve the value. That is just the supply side of it. You also have to consider the increasing user adoption and network growth of Monero. The page can be found at:

https://bitinfocharts.com/comparison/monero-hashratge.html

Here, you can see the total number of Monero transactions over the past few years. We are now at all-time highs on the metric and it appears to only be increasing. This is the utility demand for Monero. Then there's an investment case for huddling one of the premier privacy preserving cryptocurrencies. This investor demand is only likely to increase as more people realize the need for privacy coins as financial freedoms come under assault. So if we combine that steady supply schedule with an increasing rate of demand, that is all the ingredients for a price increase.

In terms of my personal thoughts on Monero, privacy is a fundamental right that we have and should not be taken for granted. Currently there's a concerted effort to erode these rights. Not just in the realms of financial privacy but also in terms of communication. This is why I am so bullish on any technology that gives us those privacy freedoms. While people may not always see the benefits of a privacy coin now, they most certainly will when they realize who has control and oversight of their personal finances. When this time does come they're going to start exploring other cryptocurrencies. Those cryptocurrencies that cannot be tracked and traced. Those that are real untraceable peer-to-peer electronic cash. I'm aware of the challenges that Monero faces. It is crypto enemy number one and there are a number of determined opponents who want to bring it down. If they cannot crack the code, then they will try to dry up all liquidity. But I don't happen to think that's likely. They've been trying for a long time. With all the resources they've thrown at it Monero remains uncracked. Moreover, the devs are some of the smartest and most idealistic in the crypto community. They build on Monero because they know the importance of financial privacy. If these devs are able to effectively implement those atomic swaps, then they could also

deal with that exchange issue. Monero is also more decentralized and efficient thanks to all the upgrades that have been pushed over the past two years. This has further expanded its adoption potential as a medium of exchange. Add to this those compelling long-term tokenomics, and you have everything you need to feel just as bullish as me on Monero. Prices are well above the 200-day moving average and general market trends appear to be positive. It's quite likely that we will see XMR above the current price assuming we get a breakthrough on the atomic swaps, then that could be much higher.

Chapter 27 Cryptocurrency regulations

When it comes to cryptocurrency regulations, it is a topic that people tend to skip, but in the same time they might be expert on how to buy any ICO-s or any Pump and Dump coins. The majority of people in the crypto space want to become rich and fast as possible, and try to avoid understanding that even if it's an unregulated market, regulations are coming to the world of crypto, whatever you like it or not. I know that most people think that the Government don't understand crypto and they can't make any changes, but you really should keep your eyes open and understand what's might be considered illegal or what isn't. But do we need regulations? Well, most people would debate this question and say that we don't need regulations, which sounds good but when it comes to scams like Bitconnect and their promoters, and think about tens of thousands of people who lost their lifesavings because they invested in a huge scam, which they dared to call cryptocurrency, maybe regulations what we need. Scam projects should not enter the open market, neither as an ICO and raising money, nor Ponzi schemes where they promise daily return which they fail to deliver. Moving on, Ponzi schemes and scams might be able to raise money one way or the other but when it comes to a trusted online exchanges selling a scam token, people start thinking that maybe that particular token is not a scam. Then later on turns out that it was a scam so who should we blame; the scammers or the online exchanges? This is another reason that SEC want's all online exchanges to register everything they sell as well making sure they have a licence to sell cryptocurrencies. There are other reasons too why regulators are stepping in. They have realized that anyone who less then 35-40 years old, just don't want to invest in any traditional market anymore such as Stocks, S&P 500, Bonds, Options or even gold and silver. Simply because the ROI, return on investment is low and slow if there is any. Instead, many people looking at the crypto space. Even traditional investment companies are trying to understand blockchain based companies and learn the knowledge required to transform their business models. Because most major companies as well private investors are heading to the same directions since 2015, this has been noticed and everyone wants a piece of it, including traditional financial advisors, banks, and of course governments. For example Venezuela already announced that they are creating their own cryptocurrency

called Petro or Petro Gold. But Marshall Island, Brazil, India and even Russia have announced to create their own cryptocurrency that they can use as an alternative payment instrument. So back to the regulations, why are they so slow before implementing any new law? Well, they have to learn about cryptocurrency and blockchain first. They have to understand what is blockchain, what is mining, how to create an online wallet and so on. Regulators have to hire experts on these topics to teach them, advise them and help them making the right decisions which that will take time. Most regulators are in the older generation too and I don't mean no disrespect, but some of these people not as familiar with technology as the current younger generation. Nevertheless, regulations are coming which is a good thing. Regulators want to differentiate what is considered legal or illegal, what are utility tokens and what are securities and so on. But who will regulate the cryptospace? Well, it's not the Police nor the FBI or CIA. Instead there are other organizations that you might never heard about so let me introduce them to you.

Chapter 28 SEC

SEC Stands for Securities and Exchange Commission, formed in 1934 in the US. The SEC holds primary responsibility for enforcing the federal securities laws, proposing securities rules, and regulating the securities industry, the nation's stock and options exchanges and other activities and organizations, including the electronic securities markets in the United States. They seem to mainly go after new cryptocurrencies and Initial Coin Offerings. But they also have reached out and publically warned online trading platforms that they must register with them in order to trade cryptocurrencies. If you visit their website on https://www.sec.gov/ go to news, then public statements, and then search for Cryptocurrencies. You can find the public statement on cryptocurrencies and Initial Coin Offerings which I would highly advise you to read. They also have a sample questions for investors considering cryptocurrency or ICO investment opportunity. For example:

- *Who exactly am I contracting with?*
- *Who is issuing and sponsoring the product, what are their backgrounds, and have they provided a full and complete description of the product?*
- *Do they have a clear written business plan that I understand?*
- *Who is promoting or marketing the product, what are their backgrounds, and are they licensed to sell the product?*
- *Have they been paid to promote the product?*
- *Where is the enterprise located?*

This is very educative, so I highly recommend you to read it.

Chapter 29 CFTC

There is another organization that you should be aware called CFTC. CFTC stands for US Commodity Futures Trading Commission, formed in 1975 to regulate futures and option markets. CFTC has designated Bitcoin as a commodity. But, fraud and manipulation involving Bitcoin traded in national commerce are appropriately within the purview of the CFTC, as is the regulation of commodity futures tied directly to Bitcoin. Products linked to the value of underlying digital assets, including Bitcoin and other cryptocurrencies, may be structured as securities products subject to registration under SEC. So to my understanding it seem that CFTC wants to make sure that no price manipulation is happening and no inside jobs on cryptocurrency exchanges. It seems that SEC and CFTC is working together to bring transparency and integrity to these markets to deter and prosecute fraud and abuse. They said that these markets are new, evolving and international, therefore they have to step in the crypto space and start questioning around making sure there are no illegal activities. To learn more about the CFTC, please visit their website at https://www.cftc.gov/

Chapter 30 FinCen

There is another organization in the corner called FinCen. FinCen stands for Financial Crimes Enforcement Network. They have formed in 1990 and their main purpose is to collect and analyze information about financial transactions in order to fight national and international money laundering, terrorist financing and other financial crimes. There was only one announcement that I heard which they said that they also step in making sure that terrorists and other financial crimes are not founded by cryptocurrencies. As you see they all seem to have different responsibilities. Maybe the SEC and CFTC works more together more closely, but I wanted you to know that these organizations already existed way before cryptocurrencies. But it seems they will be coming around and hopefully do some good use and tidy up the current cryptocurrency market. Hopefully they will get rid of the scammers from the space. Overall, regulations are good news because if Bitcoin and other cryptocurrencies are regulated it also means that they are not illegal. It is bad news for scammers, but it’s time for regulators to step in

BOOK 6

BITCOIN AND CRYPTOCURRENCY TRADING FOR BEGINNERS

MUST HAVE TOOLS, BEST EXCHANGES AND TRADING STRATEGIES

BORIS WEISER

Chapter 1 Portfolio Tools: Blockfolio

When I first started investing in crypto back in the day, I used to do it so haphazardly I opened numerous different exchange accounts and downloaded endless cool wallets to stash my absolute bizarre of unique altcoins. The problem is I pretty soon started losing track of all the crypto I owned. In fact I'm pretty sure that I still hold some coins on some old paper wallets stuck in my drawer. However things change for the better when I started using a portfolio tracking and analytics app. It was like night and day. Therefore it’s time to share with you some of the best crypto tools out there. In this chapter I'll cover the top five portfolio management tools. The pros and cons of each and I'll give some top tips on how I personally use each of them. Let's get started on my number one crypto portfolio tool is the ever popular Blockfolio app. If you are new to crypto, the chances are that you are having a hard time working out exactly how your portfolio is doing. Blockfolio basically solves that problem of price tracking and having to go through Coinmarketcap with a calculator. To get this app, please visit https://blockfolio.com/

Once you've downloaded the app from the Blockfolio website, you can add coins in just a few taps by clicking the big plus sign at the bottom of the screen. Next you'll have the option to connect an exchange account which will import your transaction history for you. Or you can search for the coin you hold and click that crypto to add it to your portfolio. You'll then be asked to manually enter in the number of coins you bought and you can key in the price you got on the exchange tot. Bash that save by the transaction button and you would have added the coin to your Blockfolio. It only takes a few clicks. Then it's merely a matter of rinse and repeat for all the other cryptocurrencies that you own and you should have your portfolio set up and tracked on Blockfolio. Why bother going through all this hassle? Well Blockfolio will automatically refresh and tell you the new value of your crypto portfolio every few seconds. It is great for those especially who wants to know what the crypto markets are doing every few seconds. This will allow you to know the true value of your crypto portfolio at any given time and the app looks pretty flashy too. When it comes to Blockfolio’s other features there is a pretty handy news function that brings together the latest crypto related articles from some of the biggest publishers all in one place. So this makes it a lot easier to keep up to date with the latest crypto news. Or to

put that another way if you're into buying the rumor and selling the news then you can use the Blockfolio app snooze function to help you with that trade. Blockfolio also has what they call their signals section. Not to be confused with trading signals. In a nutshell crypto projects push out announcements over Blockfolio signals and you'll get a message if you have that coin added to Blockfolio. What I have found is that for those projects that use Blockfolio signal service, only tend to send out the most important updates here. That saves you a bunch of time hunting through a project's numerous Twitter posts to find that super important bit of news. Finally, Blockfolio has markets section. This is basically a version of Coinmarketcap which displays key price data and market cap figures. If I click on Ethereum for example, you can see a quick chart of the price for every coin. Every coin also has a profile page. Here you'll get an overview of the coin the consensus method used, the type of token it is and what it's used for. If you scroll down, you'll find important links to the project's white paper, github, website and socials. I find that pretty useful when I'm doing a bit of crypto research on the go. There's also a plethora of additional data at your fingertips in this section of Blockfolio. This includes things like the order books and trade history on major exchanges the coin is listed on. One feature that I like to ensure I have activated is called “price alerts”. What this means is if the coin changes in value by 5% in an hour then you'll get a push notification sent to your phone. That's pretty useful to know if you're waiting to buy the dip, sell a pump or if you're trying to monitor an open position. In summary I really think Blockfolio is an essential must-have tool for anyone serious about crypto. It simply takes the complexity out of monitoring your portfolio value, scouting new coins and keeping up to date with the latest crypto news. And it's absolutely free too, so there are no excuses not to try it out.

Chapter 2 Portfolio Tools: Messari

At number two I have Messari. Although you can't really track your portfolio with it, I honestly think Messari is the best tool out there when it comes to crypto data aggregation. An essential service that helps you scout those hidden gems to add to your portfolio. In crypto, knowledge is power so when it comes to a data-driven approach to evaluating different crypto currencies or just trying to use data to make better trading decisions, then Messari is a tool you need to be looking at. It gives you numerous options to see what is trending in the space to find new coins and evaluate them. To get this tool visit https://messari.io/

If you head over to the Messari's screen then there are tons of ways you can sort coin information by clicking the columns and filters button. This will then bring up the filters panel which allows you to filter coins by things like liquid marketcap, stock to flow, on chain data metrics, sector coin category, social media stats and a whole lot more. You can get access to a ton of data filters for free, however there is some data that is hidden behind a pay-wall and to access that it will set you back $25 per month. But I don't think many people truly appreciate how useful it is to be able to sort different crypto projects by sector. With just a few clicks you can find all the smart contract platforms, stable coins, scaling solutions, payment platforms and so on. you can even put a filter on a filter and say "I don't want to trade a tiny market cap coin or anything that is a liquid" and Messari gives you the option to easily pull up that list of coins. Or, if you're a Pro altcoiner' then you can solely look at micro cap projects. Another thing is great about Messari is that they take a pretty cautious view when it comes to reporting things like the trade volume. It's pretty well-known in crypto that there are numerous exchanges accused of pushing out fake trading volume in order to gain Coinmarketcap ratings and grab the attention of traders. What Messari have done is also build a list of what they deemed the ten most trustworthy exchanges in crypto. Here you can also have a look at what Messari term real volume or just look at the reported volume from every exchange. Another cool set of stats I want to share with you on Messari is that you can get the all-time high price for all crypto assets and what is termed "the cycle low". This is basically the lowest price the crypto has reached after setting an all-time high. So with Bitcoin the all-time high was around 20K and since then

the lowest price it traded at was about 3.1K. All that is pretty useful data when it comes to determining long term bullish trends reaching lower highs. In short the way you can use Messari is to help create that short list of coins in a certain sector and with that risk profile you then typically want to see how the coin is priced today and compare it versus the all-time high and cycle low to get to a feeling of whether you are getting a decent price. From there you can dive deeper into the project and do your research before deciding what coin you want to finally add to your portfolio.

Chapter 3 Portfolio Tools: Altpocket

My next top crypto portfolio tool is called Altpocket. The tool is available for both mobile and desktop and you can use it as a crypto portfolio tracking tool, similar to Blockfolio. On your profile page you click the little plus button and add a coin in a very similar way to Blockfolio. Then you'll be given the option to auto sync your transactions from a crypto exchange or at the menu. If you are going down the manual route, you just need to key in your transaction details, hit that Add button and rinse and repeat until you've added all your coins. You'll then see your entire portfolio in the profile section of your old pocket account. That is all well and good however it's not the main value Altpocket has to offer. If you hit the best performance bar under top lists then, this will bring up the top performing traders on Altpocket according to their weekly monthly or quarterly trading performance. You can then click on their profile to see what coins they hold, the percentage weightings and see the trades they've made recently. With Altpocket you can essentially follow the top performing traders, get notifications when they make a trade and meet other traders on the Altpocket social platform. So if you've always wondered what other people are buying or selling wanted to copy trade for free or just concentrate a truly terrible trader, then Altpocket is a crypto portfolio tool you really should have in your locker. If you want to try it out for yourself you should visit the following link: https://altpocket.io/

Chapter 4 Portfolio Tools: Delta

Moving on to my fourth essential crypto portfolio tool I've got is called the Delta app. In a nutshell, Delta is a mobile crypto portfolio manager tool, much like Blockfolio. It connects with wallets and crypto exchanges to import your transactions and sends you those push notifications to alert you to the latest price movements of those coins you hold. So that means you'll have to decide whether to go up with Delta or Blockfolio. The app looks and functions very much like Blockfolio and if you want to input those crypto transactions, it works in a very similar way. Delta also has its own version of Coinmarketcap where you can check out the latest price action in the crypto sphere. When you click into a coin you'll see general data on the coin be able to view your trading activity see price alerts and order book data. Delta also has a crypto news aggregator section which will help keep your finger on the pulse of them crypto markets. There is truly not too much difference between Delta and Blockfolio and you'll be perfectly fine with either option. But Blockfolio was the first tracking app I ever used and Blockfolio leads the way when it comes to adding new features like Blockfolio signals, which Delta later cloned by launching Delta Direct. Moreover Blockfolio does seem to still be leading the way when it comes to innovation in the crypto tracking industry and you might rather get those shiny new things first than be left hanging. If you are now shore whether to go with Delta or Blockfolio, why not try them both out and see which one you personally prefer. They are free after all. If you want to give Delta for a spin then visit the following link: https://delta.app/en

Chapter 5 Portfolio Tools: Cointracking

My next pick for the best crypto portfolio tool is going to be cointracking. The way I like to think about coin tracking is that it's a crypto portfolio one-stop shop. It's got both mobile and browser-based options and offers both a paid and free version. Basically manual exchange CSV imports are pretty straightforward and fast. So the chances are that most people will never need to opt for any of the paid packages. This tool basically supports over 7,000 crypto currencies and integrates with several exchanges wallets. One really awesome feature is that you can set up coin tracking to actually watch your crypto wallets for incoming and outgoing transactions. That's pretty useful if you hate the idea of having to check your wallets every few hours to see if that transaction has come in. The Cointracking dashboard may not be the nicest looking one out there but it certainly does give you the most data. Having all this information in one place should certainly help you make better and more informed buying or selling decisions. You can also pull reports for realized and unrealized gains or losses. This is set by default to something called the “first in first out” method. But you can change the setting if you wish. The reason why this matters is that if you're a law-abiding champed, you'll be concerned about working out how much tax you need to pay. Another thing that the bean counters seem to always want to know is the average purchase price for each cryptocurrency. Cointracking makes this simple by automatically generating a report for this. I also find this type of report pretty useful when I want to work out how much of my initial investment in dollar terms I need to withdraw from a coin to let the rest right. I have no idea what the tax laws are in your country and you might also leave the numbers counting to your accountant. But if you do make it to the land of “Lambo money” then you'll have to generate a tax report. By upgrading to one of Cointracking's paid plans you can get access to the do-it-yourself tax report generator. If you do use your own account the report will save money on those accountancy fees. These types of reports make it much easier for your financial guide to work out what's been happening. I am a fan of Cointracking but I do realize that it's certainly not for everyone. Basically if you're making less than 100 trades a year then I doubt you'll get any value from the paid for plan and you're best off sticking with Blockfolio or Delta. Yet if you are doing a tons of trades and likely to have to submit tax reports,

then I go as far as saying that coin tracking is essential. If you want to check out this tool please visit https://cointracking.info/

In summary, I know first-hand that it isn't easy to manage a portfolio and make the right moves in crypto. However keeping on top of your crypto investments is a hell of a lot easier with the right tools in your locker. What I would urge you to do is try out all these great crypto portfolio tools for free and see which ones are useful to you and actually save you time. Knowledge is power and having that bigger picture of what's happening with your portfolio will help you make even smarter crypto decisions.

Chapter 6 Market Manipulation: Pump and Dump

You are being played every day in the crypto markets. There are numerous forces at work to manipulate the markets and steal those hard-earned cash. This can be incredibly frustrating for most of those traders who are just trying to break into the market. It's tough enough as it is to manage crypto market risk so adding an additional layer of risk from manipulation just isn't that fair. So how do you avoid this then? Well by knowing how to spot it. In this chapter I'm going to be taking a look at some of the most pervasive crypto market manipulation. I'll also give you some top tips that could help you sidestep those hidden landmines. Before I get into the nitty-gritty of wicked tactics, I wanted to give you a bit of an overview on market manipulation. It's not something that is exclusive to the crypto markets. Some of these have been used in traditional finance markets for a number of years. The only difference is that many of these tactics have been outlawed by the SEC. They have developed monitoring and reporting procedures which make these tactics incredibly risky for those who perpetrate them. In most developed markets the participants can pretty quickly be identified and prosecuted. The same can't be said about the crypto markets. Unregulated and mostly anonymous, those with large holdings can act with impunity and profitability. You don't know who is behind large sale pressure on a crypto coin or token. You can't identify who built up that order wall you see on the exchange. Essentially, it can be a murky old mess. Is this a massive problem? Well, yes and no. Crypto is about financial freedom. Freed from the strictures of traditional finance. It's an opportunity for users to take individual responsibility for their finances. This means that they also have to manage the risks on their own. With that out of the way let's take a look at how you manage these risks. The first and perhaps most pervasive manipulation tactic used in the crypto markets is the pump and dump. You may have heard of it but for those that haven't the impact can be severe. So what is it exactly? Well the name says it all really. Insiders or other market participants will try to pump the value of a coin until it starts gaining attention. Once other unwitting traders start jumping into the markets then the group dumps the coin on them at a handy profit. These used to be used on penny stocks back in the day but low liquidity altcoins have become a fertile breeding ground. You don't need a lot of crypto in order to pump these low cap altcoins. Moreover, a lot of these pump and dump operations are well coordinated. Users band

together in telegram groups and brazenly perpetrate these actions. Some of these groups and channels have pretty obvious names like “McAfee pump” or “rocket pump”. Some of these groups have tens of thousands of participants. Indeed it's worth pointing out that many of those who could get burned by a pump and dump are those that are late to the pump. Kind of like a game of “crypto chicken”; those who wait too late to dump their coins are left holding a bag. It's not just the pump groups. Even exchanges have gotten in the action in the past. Pump and dumps in crypto have attracted a hell of a lot of attention and have even been the focus of academic studies. For example two researchers from Imperial College London use machine learning algorithms to see whether they could identify a pump and dump scheme. How do you spot a pump and dump? Well there isn't a single data point that you can look at to identify these things. Although there are a number of factors that will add to the likelihood that something is a pump and dump. Firstly these tend to happen in low market cap coins. Most definitely out of the top 100 coins and most likely below the top 200. Pump and dumps do happen with high cap old coins but they are the exception not the norm. In the case of the research piece I mentioned, they stated that half of the pumps took place all coins that had less than 100 Bitcoin which is a pretty low cap coin. Another thing to consider is where the coin is listed. Generally pump and dump errs we'll choose those coins in which there are limited listings, preferably only one listing. This will allow them to have a greater impact on the price on Coinmarketcap. It will also mean that potential victims will have to come and buy the coins from them on the only exchange they can. Pump and dump schemes may happen on a particular exchange even if it is listed on more than one. In this case you can view it with suspicion if there is a lot of price and volume movement on only one exchange. This could be an indication that it's a coordinated action and not general market sentiment. Speaking of volume this is another really important indicator that you can use pre-pump to help you determine whether there could be manipulation. Remember that the pump and dump operators are looking to profit from it so they likely accumulated a lot of coins beforehand. If there is a lot of volume that seems to have come out of nowhere prior to a price increase, then it could be an admin accumulating the coins. Perhaps the last and most important indicator that a pump-and-dump is going is of course the price. That is after all the target of these groups. To dupe people into buying them by giving them some serious FOMO. So if you can't really understand why coin is pumping then

don't just buy it. Just remember a dump often also harms those who think they can profit from it.

Chapter 7 Market Manipulation: Order book spoofing

The next manipulation tactics I want to talk about is called order book spoofing. Order book spoofing is a crypto whales photo it's one of those gets them every time moves. So what is it exactly? Well it's basically a tactic where a market participant will place a large set of orders with no intention of ever having them executed. The market participant is trying to create the illusion of large demand or supply in the market even if there is none. It's also sometimes termed “painting the tapes”. This manipulation tactic has been used in the commodities markets for a number of years. In fact a pretty recent example is our friends over at JP Morgan who are facing a criminal probe in relation to their spoofing in the metal markets. Jamie Dimon, the JP Morgan CEO has called Bitcoin a fraud on a number of occasions. This is a tactic that has been well adopted by the large crypto whales in the ecosystem. The practice was particularly rife during the 2017 bull run, as Bitcoin prices surged to record highs. The crux of the strategy is to basically build up a large buy or sell wall on the order books of the exchange. When market participants see these order walls, they're likely to react to them. I mean if you see a cell wall of over 1,000 Bitcoin on an order book, that's likely to spoof your analysis. Are you likely to buy Bitcoin if you think that it won't break past a cell wall? Probably not. However in the background the whale is secretly accumulating Bitcoin while the market hits those sell orders. Then as if it came out of nowhere, you'll see that the cell wall evaporates into thin air. The whale then pulls his order knowing that his deed is done and the market has been fooled. This can of course happen on the other side of the trade as they build up those large buyer walls. You think that there is support to hold up selling pressure. This creates some bullish sentiment among the rest of the market participants. You go long on Bitcoin expecting that the Bulls have the edge until you realized that those bulls were nothing but wolves in Bulls clothing. And the opportunity to profit from spoofing becomes that much more lucrative, when these same whales take positions in the Bitcoin futures market. They can profit from volatility in a derivative market, where they are manipulating the price discovery in the underlying market itself. It really is a fascinating tactic. Devious, but fascinating.

Chapter 8 Market Manipulation: Wash trading

The next market tactic that I want to look at is a variant of spoofing and it's called “wash trading”. Wash trading is a tactic that's used in order to create the perception of an active market in a particular asset like the other tactics mentioned previously. It's illegal in established financial markets but appears to be fair game in the crypto space. It usually entails the simultaneous buying and selling of the same asset by one individual or between a group of individuals. The hope is that it creates an illusion of volume in the asset itself. In general, traders are more likely to trade a cryptocurrency that has more volume and hence liquidity than those that do not. Of course this volume is nothing but a facade and those traders will soon discover that the underlying liquidity is not there. Those who take part in the wash trading are usually either specific crypto projects or those backing it as well as the exchanges themselves. This was actually brought to light in 2019 by a Russian coder who developed BOTS to fake exchange volume. This is all done in order to pump the volume numbers on Coinmarketcap. This duped the newbies into thinking other people a trading the coin or using the exchange. This is actually a pretty important point that has been raised on countless occasions. Those volume numbers that you see on Coinmarketcap are not as they appear. There was actually a pretty interesting presentation by Bitwise Asset Management as an SEC hearing in 2019. They claimed that over 95% of the volume is fake or non-economic in nature. Although CMC have been making a concerted effort to improve their filters. So how do you spot a wash trading on an exchange? Well, perhaps your first bet is to avoid dodgy exchanges. There is now such a large selection of reputable exchanges that should have the coins you want to trade. There's no need for you to use some bucket shop operator out of an offshore location. You can also then look at the order books of suspicious exchanges in order to spot the faking. The tell-tale signs of faking are an almost uniform pattern of buy sell orders. You'll also notice that on every time stamp you have a matching pair of buys and sells. These trades will also be roughly equal in size so that both the buy and sell match. Then when it comes to the order sizes in general, they're quite random and have never less than a certain threshold. Finally, if there is a pretty large bid ask spread on an exchange that is supposed to have high liquidity, it's usually something you should be cautious of. Also sometimes these things come down to a bit of gut feeling. Should some obscure unheard of exchange really be doing almost as much volume as coin based Pro? It also helps to do your own research. Tap the community to ask their opinions about particular

exchanges. There are some that are known to be unreliable at best and complete scams at worst.

Chapter 9 Market Manipulation: Stop loss hunting

Sometimes crypto whales like to go hunting for all of those stops. Stop loss hunting is a tactic that used to force market participants out of their positions by driving the price of an asset low enough so that it triggers their stops. The hope of the whale that is using this tactic is that they will be able to pick up the asset at a lower price. It's just using your significant market influence in order to force the hand of other participants. Also most traders will tend to place their stops at key technical levels. Absent of any market manipulation, these levels generally tend to signify key capitulation points. So the whales have an idea of where to target when they're pushing the market down. Let's take a look at an example.



Here is some unidentified altcoin on Bitfinex. Let's call it example coin. The Green Line is where the stops are positioned. Whales love it and want to stock up on example coin so they execute a whole host of cell orders and push the price towards the stops. Once it reaches key technical levels, a host of automated sell orders hit the market and the well can scoop up his example coin. As you can see the market recovers almost immediately as the whale buys the example coin and other market participants realize that it's going on the cheap. You on the other hand wake up to discover that your stops were hit overnight and the price is where it was just before you went to bed. So how do you avoid being the prey in this hunt? Well this is a bit tricky. You still want to be placing those stops as these are essential to manage risk. More likely than not the market is legitimately moving down, and you'll want to protect your downside risk. But what you could try and do is place a stop limit order. These are basically stop orders that will have an execution price above the trigger price. So once the market goes through your stop limit sell

orders will be placed a few points below the stop level. The benefit of this is that you're still protecting yourself from large downside risk. However you are leaving a bit of room to confirm that it is indeed a legitimate capitulation point. There are a number of exchanges that offer variants of stop limit orders. If you're trading futures then buy what they call conditional orders. Stop hunting is a really intriguing market tactic.

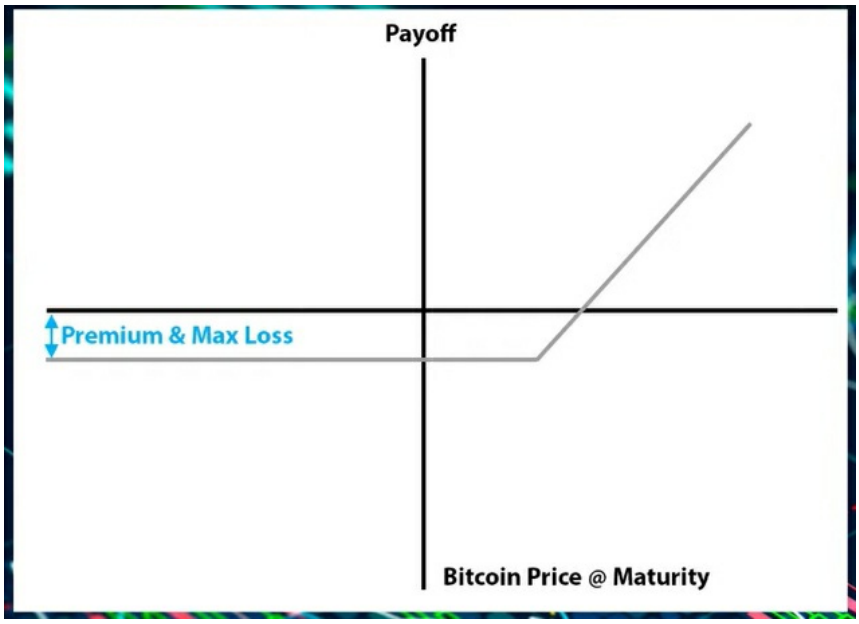
Chapter 10 Market Manipulation: FUD

Another market manipulation tactic is called FUD. FUD stands for Fear, Uncertainty and Doubt. It is often one of the most effective ways to move a crypto assets price without actually buying or selling anything. Crypto traders can be pretty jaded and negative news sends them for the hills. It's actually a well-known psychological heuristic that human beings have a strong aversion to loss. In fact they feel more upset by taking a loss on the downside than they feel good about taking an upside profit. Traders hate taking losses, hence if you create a fake news narrative around a project of some sort, then you can have a pretty large impact on the price. Sell the rumor and buy the news. Propagating false information is used with great effect by many long/short equity hedge funds. They will usually push false information about a company just after they've taken a sizable position on it. Out of all the other tactics spotting fake news in crypto can be quite a difficult endeavour. The whole crypto news space is filled with so much junk that it's really hard to filter. A lot of it will have to come down to your own judgment. Is the source reputable? Are there facts to back up the claims? Is it being pushed by known trolls in the space? Could the trolls have an ulterior motive for spreading the FUD? Also, you don't want to fall into the category of person who dismisses everything as FUD sometimes concerns are legitimate and they will likely manifest themselves in a useless project. Let's not forget that many of Bitconnect connections were at some point shouting “FUD“.

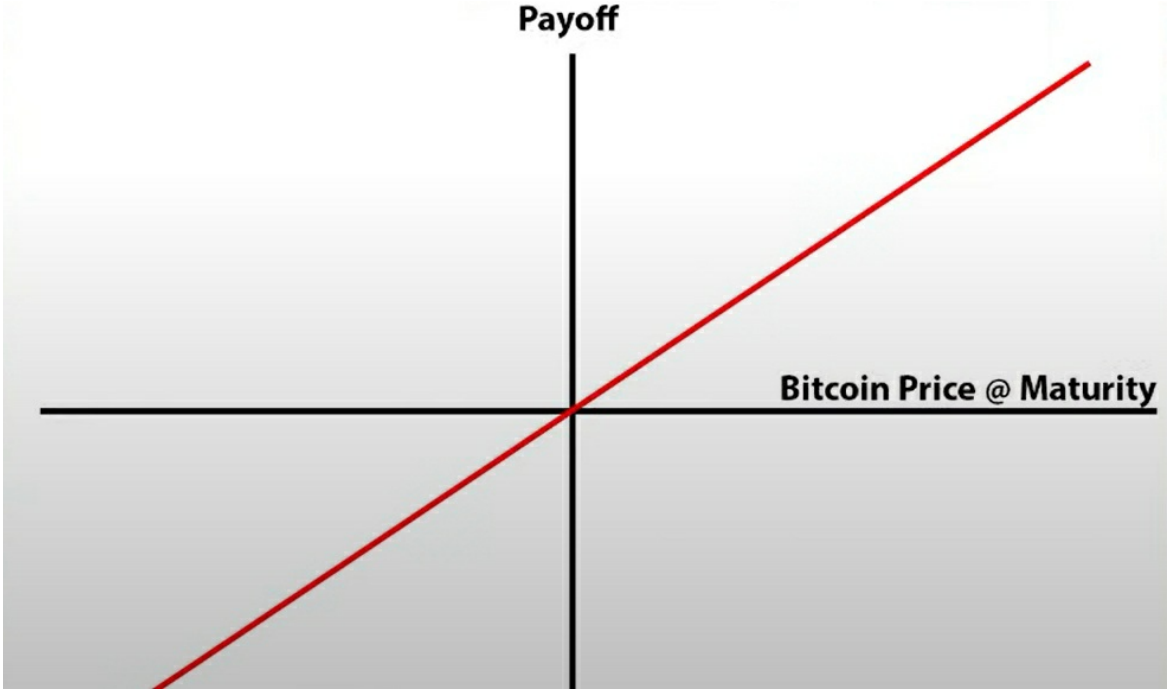
I hope I haven't deterred you too much from trading in these Wild West markets. The truth is that they are becoming much less lawless these days. Most of the reputable crypto exchanges won't allow some of the tactics on their platforms. Moreover, even though there's no crypto trading regulator the CFTC and SEC have taken notice. Both of either issued consumer advisories or pursued legal cases against miscreants. In any event, it's important that you're aware of these tactics so that you can avoid these potholes.

Chapter 11 Bitcoin Options: Option Theory

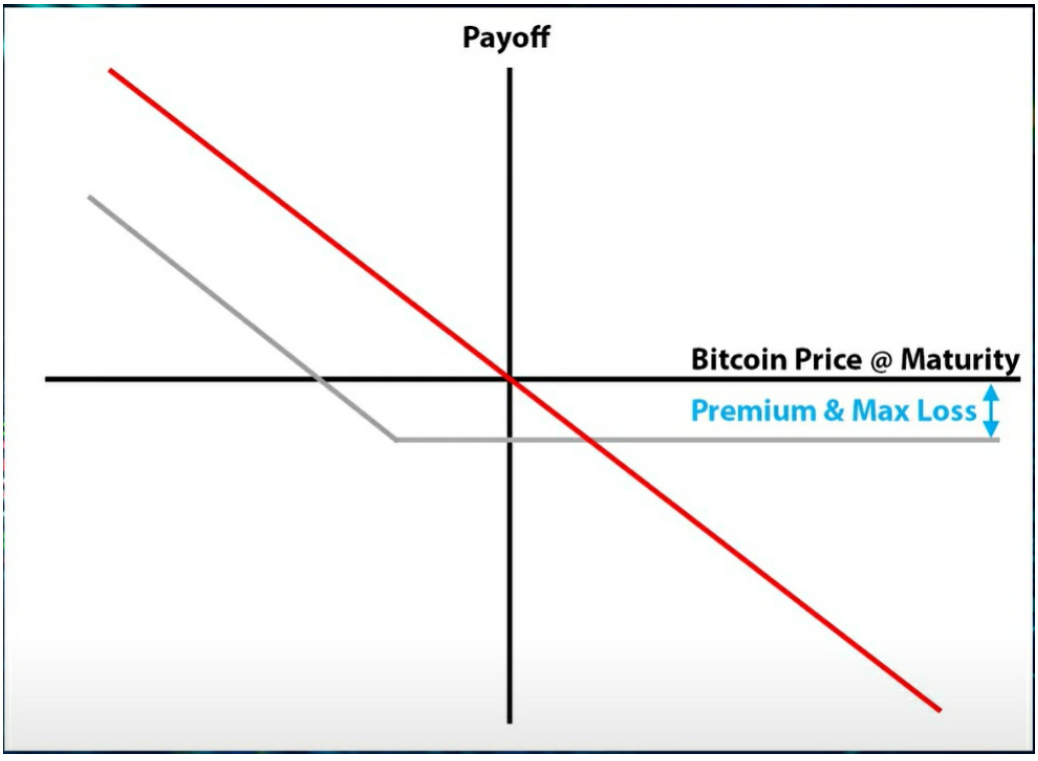
As the Bitcoin markets evolved, the number of ways in which you can trade it does too. I'm sure you all know about the numerous futures markets out there, but did you know that Bitcoin options are being offered on an increasing scale. These instruments can open up a whole range of trading strategies you didn't know about. In the next few chapters I'll be going over what exactly Bitcoin options are, how you can use them to protect your portfolio, where they're currently being offered and my personal view on where the options market is headed. Before I can take you through any sort of option trading strategies, I have to lay the groundwork. So what exactly are options? Well their name says a lot of it. They confer on a holder the right but not the obligation to buy or sell an asset at some time in the future. When you enter a "call" option, it's the right to buy and when you enter a "put" it is the right to sell. They differ from futures instruments in that futures have an obligation to buy or sell the asset that you've entered a trade for. Basically with an option if you find that exercising the right to buy or sell is not profitable on expiry, you can let it expire worthless. With a future you have to either cash settle it or buy / sell it. This means that options are instruments with asymmetric payoffs. What do I mean by that? Well look at this graph of a simple call option.



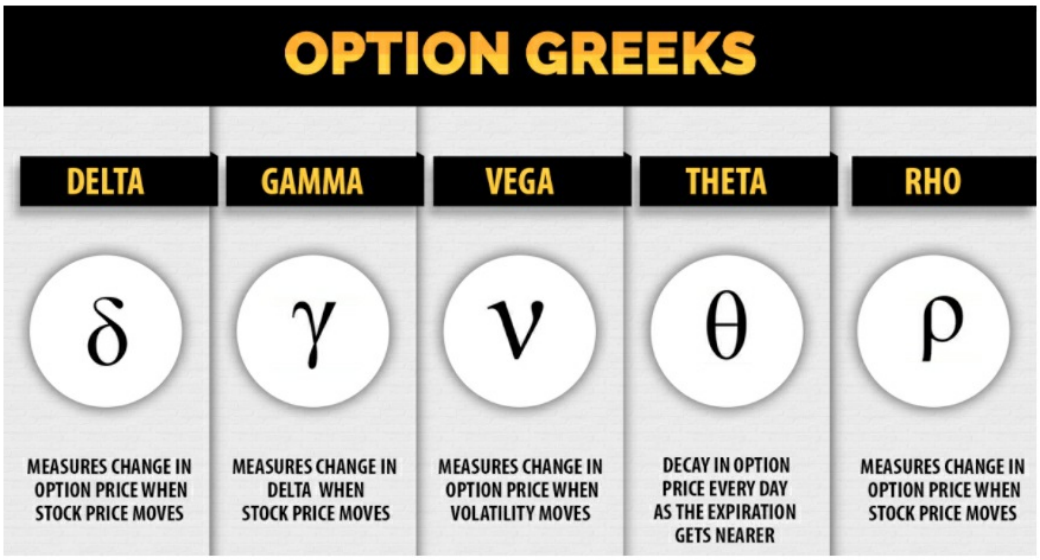
And now look at the graph of the futures instrument;



Well, you can see that your loss on this trade is limited only by the option premium or cost of the option. You can't lose more than you've already paid. With the future on the other hand your potential loss is unlimited. Or take a look at this graph of a put option and now overlaid with a short futures contract.



Same thing on the downside. If the price of Bitcoin rallies you have a maximum loss with the put option whereas you have an unlimited loss on the short future. This is more applicable to the listed and OTC future varieties. Leverage futures trading exchanges will be quick to liquidate you to prevent negative equity and hence limit your downside. There's also another side of this option crypto coin. You can also sell options. This of course limits upside and could lead to unlimited losses. Why would anyone sell these you ask? Well, they can form some pretty unique trading strategies with them, something that are covered in a bit. Before I get onto that, I need to cover some option theory. So let's dive into the deep end and be sure to pay attention so as not to drown in maths. When it comes to options there are a number of variables or inputs that impact on its value. These are the strike price, the spot price, the time to maturity, the underlying implied Bitcoin volatility and the risk-free rate. The strike price is the price at which you agree to buy or sell the option in the future. The spot price is the price right now. Time to maturity is how long the option has to go and implied volatility is a measure of how risky the market is. Each of these factors impact on the value of the option in their own unique way. The difference between the strike and the spot has perhaps the most direct impact on value. However holding other factors equal, the higher the volatility the more valuable. The longer the times and maturity the more valuable. These variables or inputs are often labelled the Greeks.

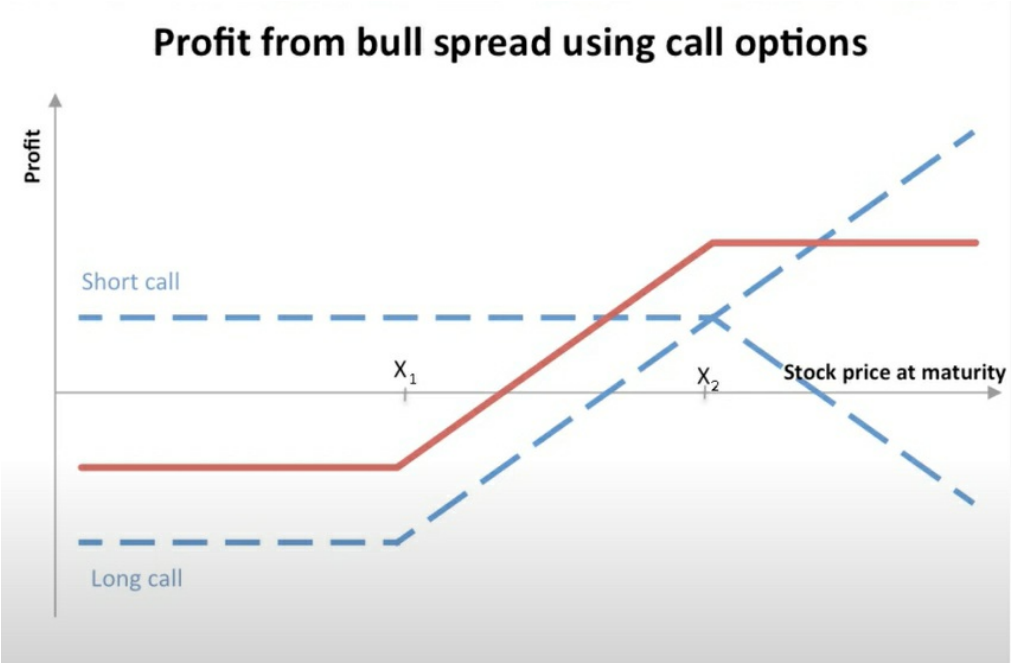


They called the Delta, Gamma, Vega, Theta and Rho. The exact mechanics and maths behind these inputs can be quite complicated. There is one more

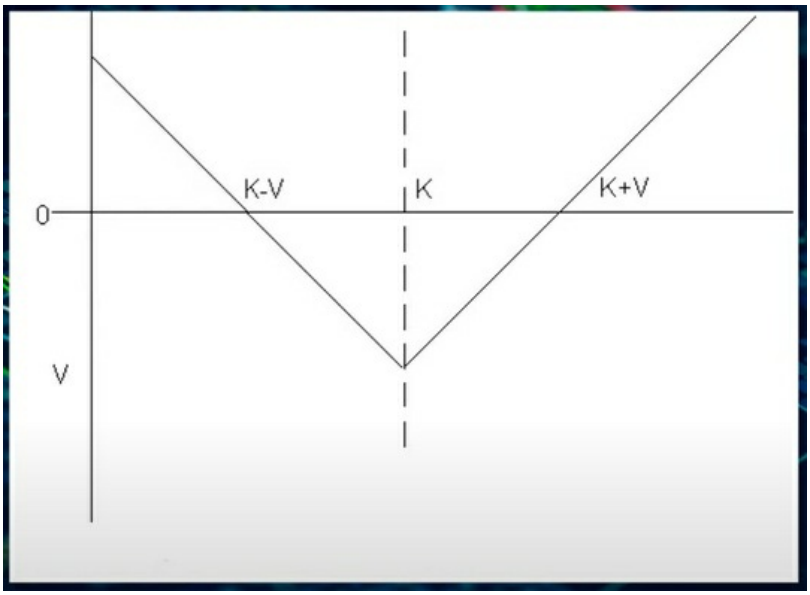
thing that I briefly need to discuss and that is the “moneyness” of an option. It's that relationship between the spot and the strike price which has the biggest impact on the options value. Simply put an option could be in the money, at the money or out of the money. Here is what they mean. In the money is when the spot is above the strike for a call option or if the spot is below the strike for a put option. Out of the money is when the spot is below the strike for a call option and vice-versa for a put. At the money means the strike equals the spot price. I should also point out that these all assume the pricing of plain vanilla European options. You also have way more exotic variants that won't be covered in this book. Now have a vague understanding of options let's dive into options strategies.

Chapter 12 Bitcoin Options: Option Strategies

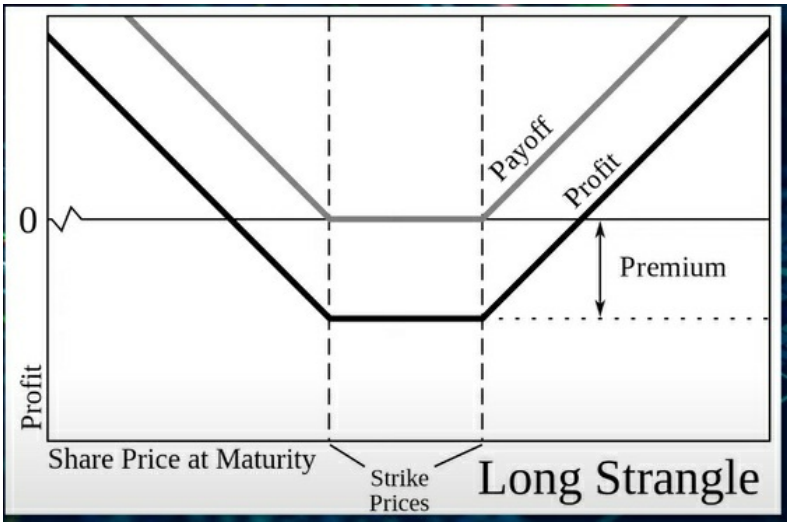
Given that options have an asymmetric payoff, you can structure some pretty unique strategies with interesting payoff profiles. For example, assume that you're bullish on Bitcoin in the short term and would like to go long. But you don't think that it will really moon beyond 14k by the end of the quarter so instead of buying a simple call option, you could buy a call option and finance part of that cost by selling a call option with a higher strike price. This is called a "bull spread" and has both an upside payout and a downside loss. The difference between this and a simple call option is that you have a lower downside loss. This bull spread can be done for a downside bearish trade as well.



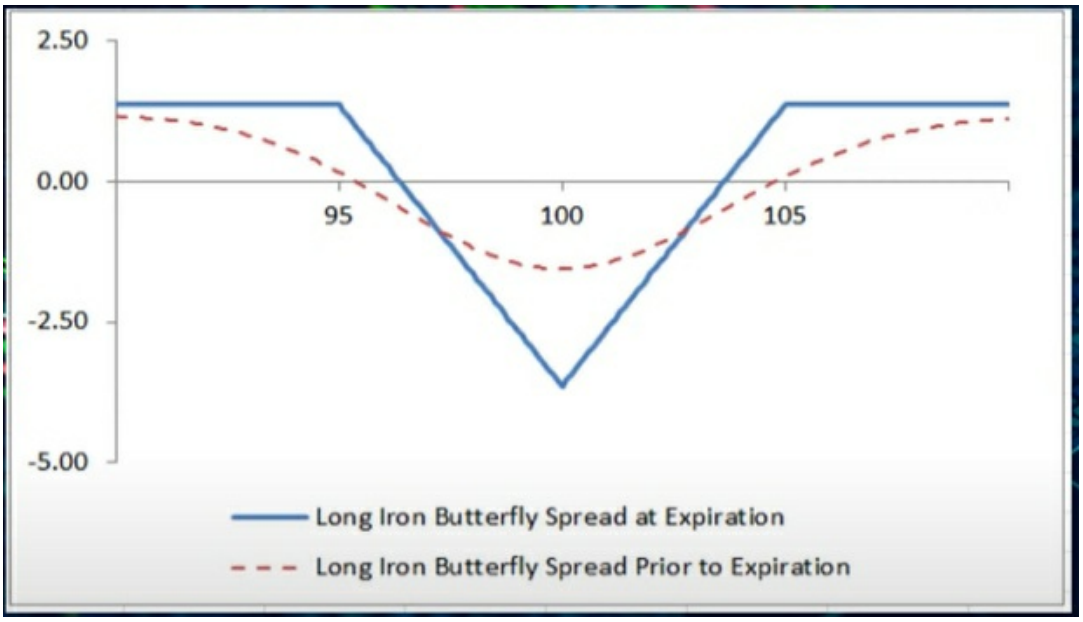
Here is a bear spread we're a short put option decreases the cost of the short. Or how about if you don't really know where Bitcoin is likely to go but you are certain that it will be incredibly volatile in the next quarter. It could moon or it could tank. You could then buy both a call and a put at the same strike price. Here you have what is called a straddle.



If the price moves dramatically, either way, you get a decent payout. Of course buying two at the money options could be costly so you could buy a call and a put that are both slightly out of the money. What you have now is a strangle and this is your payout.



Or how about you sell away the upside on both options with two more options. You now have what is called an Iron Butterfly and it guarantees you a certain payout if Bitcoin rallies or tanks. It can also be called an iron Condor when done on a strangle.



What about if you perhaps have the view the Bitcoin won't move anywhere for a couple of months. Well then you can also sell straddle or strangle your play here is that volatility remains low. You can also limit your downside by buying another call and a put. These are only a few of the strategies and spreads that you can design. You can also build something called “calendar spreads” which structure options with different expiry times.

Chapter 13 How to build options strategies on Deribit

I'm sure that you're wondering where you can buy these options so let's take a look into that. When it comes to the market for Bitcoin options, they are far less developed than the futures markets. Yet, there are a number of places in which they are offered. There are three types of market where Bitcoin options exist. Through swap and option dealers like Ledger X. Listed on an exchange such as the CME Group or Bakkt. On retail exchanges such as Deribit.

To get to the Ledger X's website please visit: https://www.ledgerx.com/

To get to the CME's website please visit:

https://www.cmegroup.com/trading/options.html

To get to Bakkt's website please visit: https://www.bakkt.com/bakkt-markets

And to get to the Deribit's website please visit: https://www.deribit.com/

For traders perhaps our best place to buy these options is on Deribit. This is a crypto Deribit platform that has been around since 2016. It's quite popular and also offers perpetual and quarterly futures contracts. But we're interested in their options instruments. They currently have two markets for options; Bitcoin and Ethereum. I'd rather opt for the Bitcoin options as these have the most liquidity. This option exchange works much the same way as traditional exchange order books, except that there are numerous markets. The markets will differ according to whether it's a call or put, the expiry as well as the strike. You can bid or offer options in order to build your required strategies. Let's build a strategy right now just to give you an idea of how it would work on the platform. What strategy should we build? Well, I'm bullish on Bitcoin in the next three months but don't think that it will rally much above 12 K. So I'll build a bull spread. A simple bull spread requires two call options; one long and one short. I'm going long a call option on 10 Bitcoin with a strike of $10,000. On the order form it implies a price of about 0.08 Bitcoin per option or 0.8 Bitcoin for the ten Bitcoin. With these options if Bitcoin is below 10K at the end of the next 3 months, I will have a loss of the 0.8 Bitcoin I put up. Still a pretty good sum. However I can reduce that potential loss by selling away a bit of the upside with a short call option at $12,000. Both of these options have an expiry in three months which is the time frame for my trade. Once orders a place and executed, my trade is live. There is something to

point out here. The options under a bit are marked to market constantly. So your bull spread PNL will constantly be adjusted to reflected. You'll also have to put up a sizable margin for the short position as well. This is just so that Deribit can manage the risk posed by short options in general. On expiry of the trade your bull spread should have the same payoff as you pictured in your payoff diagram. Setting up any of the other strategies, works in the same way. Be sure to match the expiry and then you can choose the strikes that are needed for the strategy. For strike prices that are far away from the money, you may struggle with liquidity. This is just a factor of it still being a relatively new market.

Chapter 14 Extensive potential for Option markets

Let's now discuss the broader potential for crypto options. One of the biggest markets for crypto options has to be from institutional investors and miners. The letter to finance operations and the former to protect or enhance crypto portfolios. Previously, large option contracts used to only be traded over-the-counter or through swap dealers. Dealers such as Ledger X structured bespoke option deals that saw some hedge fund traders make millions. These options had a strike price of $50,000 and an expiry date at the end of 2018. The problem with these OTC option contracts is that sometimes the dealer can't find a counterpart to their trade. The OTC market is chunky and idiosyncratic. This is where Exchange listed option contracts have an advantage. These markets are more liquid as the contracts are standardized. Hence it's a lot easier for institutions to structure trades. Bitcoin options are now being offered in listed form on a few exchanges. In December of 2019 trading began on quarterly Bitcoin options are Bakkt. Bakkt was the first regulated futures exchange to offer physically settled Bitcoin futures. In January of 2020 the CME announced the launch of their own listed Bitcoin options contracts. There was a lot of anticipation for the launch of these options as open interest in the CME futures markets spiked just before the rollout. On the first day of live trading, volume on the CME exchange exceeded all the volume that was traded on Bakkt since its launch in 2019. What's driving the demand? Well it's a number of things. Firstly, given that these options settle into CME Bitcoin futures, traders have another unique way to profit from the future settlement dates. They construct your option trades around these highly volatile dates. We also had the Bitcoin halving and the potential volatility this have thrown up in the Bitcoin markets. While this is only Bitcoin options right now, we could also see Ethereum enlisted contracts in the not-too-distant future. This is because it seems as if listed Ethereum futures are about to hit the market. Given that Bitcoin options followed the Bitcoin futures, it is not beyond the realm of reason to expect the same from Etherium. What could all these options mean for the Bitcoin markets? Well, options are less of a speculative instrument than futures are. They're a great way to hedge risk in an inherently volatile markets such as Bitcoin’s. By reducing risk it could temper volatility. There is strong evidence that the introduction of option instruments to the FX markets have a

calming effect and brought down the wild swings that it used to have in the past. As we know, one of the primary arguments made against Bitcoin is that it's too volatile to be used as a medium of exchange. If more stability is brought to the market, could we see more adoption of Bitcoin or crypto from the reduced volatility? Well, not sure. We are also hoping to see more retail exchanges offering crypto options which can be used by most of us. Although they're slightly more complicated than futures they give us a more sophisticated and less risky way to trade the markets. They're also more of a risk management tool than a form of speculation. If we take a look around crypto trading circles these days, it appears to mostly be centred around multiplying an investment rather than preserving a portfolio. Another thing that we're likely to see pretty soon is decentralized options built with smart contract technology. Already there are a number of projects that are building blockchain based solutions for derivative instruments. In other words we could one day see decentralized option exchanges. Think 0X (ZeroX) or Kyber Network but for bespoke option contracts. Defy option contracts built on the blockchain and traded on chain. Immutable, transparent and in your hands.

I'm really quite excited about the opportunity presented by Bitcoin options. Firstly it's going to further credential eyes Bitcoin markets in the eyes of the institutions. With a regulated and liquid options market, these big funds are more likely to dip their toes in. It could also provide an important risk management tool, not only for these funds but also for those businesses that rely on Bitcoin. Miners could write contracts to hedge Bitcoin risk for future mined Bitcoins. By providing certainty of cash flows it could encourage more capital investment today. As these options bring more certainty and security to the Bitcoin markets it could quell some of that intense volatility. A more stable Bitcoin is a better outcome for all. No longer will you have to hear the argument the Bitcoin is too volatile as a currency. Moreover, if Bitcoin options turn out to be a success then it could open up the possibilities of numerous other cryptocurrency options. There are a whole host of more exotic option types that exist in the financial markets. If vanilla options on Bitcoin turn out to be a success, we could see more exotic variants eventually being launched. Could we see American options or maybe the digital variant? These are advanced options with unique payoff parameters. They're regularly priced in traditional financial markets and they provide their own unique benefits. Indeed, there may be an OTC broker right now that's already

facilitating deals of more exotic cryptocurrency options. If there's one thing that we've learned it's that dealers will line up to provide markets as long as there is demand. Liquidity is increasing and efficiency is on the rise. Volatility is decreasing and ignorance is on the decline.

Chapter 15 Crypto Trader TAX tool

There is a major problem. Crypto taxes are complicated and most accountants run for the hills if you even whisper the word Bitcoin. It's all too tempting to stick your head in the sand and pretend those sick games never happened. But eventually those gains need to be accounted for. In the following chapters I'll go over a few crypto tax software solutions. I'll explore the pros and cons of using them and tell you about all of their features. First, I'm just going to give you a brief overview on why you might consider using crypto tax software. If you finally managed to pick that hot altcoin and land it on the moon, you have two choices. The first is to try and cash out those crypto riches and hope those annoying tax men don't notice. The second option is to get those taxes calculated and work out how much to hand over to the government. Many people think that taxation is legalized theft and they have to keep a low profile to avoid paying them. But if you enjoy getting a good night's sleep you might be wondering why you need to use crypto tax software. Well, you don't. You could go through all your trades manually look up and apply the tax guidance for the country where you're based. It's all very possible to do yourself. The problem of course is that recording and ending up every single trade to work out your gains and losses is phenomenally time-consuming. Things get even slower if you're not a professional counter. I imagine that you value your time and don't want to spend weeks working out how much tax you need to pay. That's where crypto tax software tools come in to do the heavy lifting for you. Put simply, all these tools really do is save you time and stress when it comes to reporting that tanks. Nothing more and nothing less. With all that said, let’s take a look at what options you have in terms of crypto tax software. There is a software called CryptoTrader.Tax. What it does is provide crypto traders and investors with a lightning-fast way of calculating their capital gains, losses and tax owed. This option is mainly geared to the US market but there is international support to and taxes can be calculated for any country that accepts the FIFO and LIFO standards. All those calculations are available in almost any fiat currency too. What does crypto trader tax have in terms of features? Well it comes with a simple to use tax file. This is how it works. You need to create an account import those crypto transactions from your exchange accounts using the API import tool or you can alternatively just upload the trade history CSV file. So which exchanges are actually supported? Well, there are several really but to get a

complete up to date list please visit their website at https://cryptotrader.tax/

Once you've imported all your trades you will then have to add the source of that crypto income over at the current tax year. The good news is that this tax platform can work out gains made by a ton of different crypto specific sources. Things like mining, forks, air drops, staking and even gifts. Finally, you'll be asked to select your chosen tax calculation method and the tax form you want to be generated. Basically CryptoTrader.Tax will then spit out a tax report that includes a bunch of documents including things like an income report, the 8949 IRS form, an audit trail report and a short and long term sales report. You will also get an end-of-year positions report and a TurboTax online direct import file. What that means is that you can then import that report into other conventional tax tools like Turbo tax or Tax act. Another cool thing about CryptoTrader.Tax is their tax loss harvesting feature. That means you'll be notified about cryptocurrencies that offer a solid tax saving opportunity and this leads to better long-term tax planning. For those wanting their report looked over by a qualified accountant before submitting it to the government, the tax platform also allows for accountants to import review and far tax reports on your behalf. Pretty useful if you want things double-checked for you. So what will this tax software solution cost you? Well the hobbyist plan is priced at $49 per tax season. That includes imports of up to 100 trades, free report previews, live chat support, unlimited revisions, IRS forms, cross-platform integration with tax filing software like TurboTax, tax loss harvesting, FIFO and LIFO computing. The day trader plan gives you all that and support for up to 1,500 transactions for $99 a year. The high-volume trader plan supports up to 5,000 trades, unlocked premium customer support. For $199 you can get unlimited transactions supported for $299 per tax season. If you wanted to try it out for free with limited features, then you can do that too. If you're in the market for a crypto tax software tool, I'd highly recommend it. But what are the pros and cons of CryptoTrader.Tax? Well you should certainly have this crypto tax tool on your shortlist if we are looking for a tech solution that has an intuitive interface, is easy to use and offers a free trial. I'd also recommend this option if you're based in the US given their focus on that market. For the cons I'd like to see more exchanges support it and you should be aware that the platform focuses heavily on the US and IRS forms. That means that there are better options for those based elsewhere in the world. Finally who is CryptoTrader.Tax for? In my opinion this tax solution is ideal for anyone filing crypto taxes in the US but there is

limited leverage trading platform support. So if you're into that then you'll probably need to look at other options. All that being said, it's quite straightforward and beginner friendly. So if you're new to the world of crypto tax calculations then this is a great place to start.

Chapter 16 Bear.Tax tool

The next Tax Tool I recommend you to check out is called Bear.Tax. This tax software solution offers users a quick and easy way to compute and file those tax reports. Like CryptoTrader.Tax, it's designed primarily with the US market in mind and is usable in other countries too. Bear.Tax was built for average consumers in mind as well as for financial advisors so you'll have no problems when it comes to sharing those reports with your accountant. How does it work? Well Bear.Tax takes a similar approach to other competitors. This basically involves importing your trades either by API integration or uploading a CSV file of your trades. Yet you can then select if you want to process your report using the FIFO or LIFO rules. Finally the software will also generate those tax documents for you. When it comes to income classification, Bear.Tax offers a little more choice than CryptoTrader.Tax with support for income sources like gifts, staking rewards, airdrops, hard forks, referrals, mining voting rewards, community rewards, inheritances crypto payments and earning programs. So if you've got involved with an income source that's not supported by CryptoTrader.Tax then you'll probably want to look at Bear.Tax instead. Another great thing is that the platform smart matching algorithm helps ensure that transactions are recorded and processed without taking fees and block time delays into account. That helps ensure compliance with IRS guidelines through recording taxable events whilst also ensuring that you do not over report tax. Pretty efficient. For those that HODL-d and didn't really think about all this tax when they started, Bear.Tax has you covered with a transaction review function. This allows you to search specific transactions and make modifications. That means you can ensure that you input the correct cost basis for a specific time or date. If you initially refused to pay for a crypto tax software tool then you'll know all about the pain of scrolling through Coinmarketcap graphs to look up the price of a coin in the past. That is now a thing of the past with Bear.Tax which offers historical pricing data for every supported cryptocurrency. Another thing to know is that this software tool also supports high-frequency traders and BOTS. So if you've used a BOT like three commas to help automate your trading then Bear.Tax is going to be one of those tax tools you want to look at. Bear.Tax supports many exchanges but to get a full view, please visit their website at https://bear.tax/exchanges.html

If you're only place a few trades per year then the basic plan will have you covered. Price is just ten dollars per tax year this option supports up to 20 transactions and unlimited exchanges. The intermediate plan will set you back forty five dollars and is good for 200 transactions. Plus you'll get access to email custom support too. The expert plan is for those that hold multiple exchange accounts with up to one thousand transactions supported and you'll get chat support as well. Finally the professional plan is two hundred dollars per tax year. For that money, you get unlimited transactions, unlimited exchanges, priority support, custom file imports and the ability to connect with a qualified accountant. When it comes to pros and cons, and massive Pro is how keenly priced Bear.Tax is. The pro plan is a great value and is ideal for those that wants an accountant to look over those tax computations and ensure everything is well. I also like how the basic plan is only ten dollars and how that should cover most HODL-ers who only do a few trades a year. That 10 bucks seems like peanuts when it comes to making your life easier. All that being said a lot of people do trade on the likes of BuyBit and Bear.Tax doesn't support that exchange. So if that's you then I'm afraid you're going to have to look at other options. Who is Bear.Tax for? Well, it's for anyone who wants a cost efficient tax automation tool.

Chapter 17 CoinTracking as a TAX Tool

The CoinTracking software is packed with top tax reporting tools to help make filing those taxes a breeze. There's a huge amount of data available on CoinTracking and that includes things like a personal portfolio analysis, trade imports, tax declarations, coin charts and coin trends. CoinTracking is very popular. It has over six hundred and ten thousand active users and over 750 CPAs and corporate clients. This tax software solution is responsible for generating tax reports for portfolio holdings worth 4.3 billion dollars. If you're a crypto OG then CoinTracking has you covered with 11 years of historical price data. Also altcoin dumpster divers out there will be covered seeing that CoinTracking supports over 7500 coins. The cool thing about CoinTracking is that it's suitable for both crypto traders and businesses. So if there are any budding crypto entrepreneurs out there, you will probably want to take a closer look at this option. Here's how it works. CoinTracking basically crunches the numbers for you once you import your trades and spits out a plethora of data like real-time profits, losses, coin value, gain, taxes owed and more. The personal portfolio analysis feature includes a series of interactive charts for trades and coins audit reports for profits and losses as well as an overview for realized and unrealized gains. Overall, 70 exchanges are supported by CoinTracking and a full list can be found at their website:

https://cointracking.info/

Another cool thing is that you can import wallet data from the likes of Leger and Trezor and there's also support for a host of legacy exchanges. Even MTGox. Like every crypto tax software tool on this list you can connect two exchanges using API integration to import those crypto transactions. However direct blockchain network sync is also available. Unlike Bear.Tax and CryptoTrader.Tax, CoinTracking has a load more tax computation methods. Well, 12 of them. That does include the standard FIFO and LIFO methods as well as the average cost method and many more. What all that means is that CoinTracking is compatible with more tax jurisdictions than any other solutions I mentioned before. If you've ever done your own taxes before you'll only know too well the problems you get into when there are missing or duplicate transactions. Basically things don't balance and that means you need to go through every transaction which is time-consuming. That should be a thing of the past with coin tracking as the software has

several methods for verifying transactions designed to discover those missing or duplicate transactions. When it comes to cost coin tracking it has a pretty good free option that supports up to 200 transactions, limited reporting for tax and capital gains, coin tracking and CSV imports. You should definitely try before you buy this tax software to make sure you're happy with it before committing. Here's the thing you need to know about paid for plans. They are charged monthly and not per tax season. The pro plan supports three and a half thousand transactions, prioritized transactions and gives you access to customer support for 10 dollars a month. Level up to the expert plan and you get everything in the pro plan and support for up to 20,000 transactions. For $50 a month you get support for unlimited transactions and prioritized customer support. I want to move on to the pros of CoinTracking. It supports 12 different computation methods to calculate crypto tax and that means it's built to directly serve a wider range of countries. So if you're living outside of the US then you probably to look at this option. A ton of coins and exchanges are also supported so that means that this solution is ideal for both pros altcoiners and leverage traders. When it comes to the cons, the paid plans could be pretty expensive. If you've only made a few trades over the year I'd recommend you look at a cheaper option like Bear.Tax. So who is CoinTracking for? Well, it's one of my top choices for anyone living outside of the US, who has a bunch of transactions over the tax year. If you are a leveraged trader using buy bit or a low cap altcoin then this is the tax solution you should definitely be looking at.

Chapter 18 Koinly TAX Tool

My top crypto tax software pick is called Koinly. Why does it deserve the number one spot? Well unlike so many tax software solutions this one actually doesn't focus on the US alone and boasts full support for over 20 different countries. That includes support for the US, Canada and the countries in Europe. Asia has some support for Japan, South Korea and Singapore then you also have support for Australia and New Zealand too. I personally found Koinly portfolio analysis tool extremely useful when it came to truly understanding my portfolio. It has handy tools that allow you to view the ROI on each crypto investment invested, Fiat income, profit loss and capital gains. This means that there's no hiding from your losses whilst making it very clear you actually made some pretty smart moves. Another awesome feature is that unlike the other tools mentioned, in Koinly these data import function doesn't require you to bounce back and forth between multiple exchange accounts. That automated data import can be through a standard API exchange connection or by simply adding a cryptocurrency wallet address. What Koinly does with that wallet address is use a smart transfer matching system which leverages artificial intelligence to detect transactions made between your personal wallets. That's handy because no one wants to pay taxes on transactions sent to themselves. What's even better is that data on margin trading, futures trading, staking, lending and defy can also be imported. So once that transaction data is imported in Koinly what's next? Well generating your tax report of course. The great thing in Koinly is that you can preview those reports for free and those annoying tax forms are auto generated by Koinly for you. That includes things like IRS tax forms for those based in the US. International tax reports are also available for those based in countries like the UK, Canada, Germany, Sweden and more. For those that use TurboTax, then you're all good here as Koinly has data export functionality that's compatible. If you don’t like going through a ton of transactions to find missing or duplicate transactions, the good news is that Koinly has several tools designed for just that job. That even gets better when it comes to compatibility. Koinly supports over 350 crypto exchanges, 50 wallets, 6000 different cryptocurrencies and even supports crypto services like Lending block, Block by token, Set Blockfolio and more. In short, Koinly has the best support of any tax software tool I found. What's the cost

of all this? Well unlike many of its competitors Koinly offers a very functional free plan. This includes support for 10,000 transactions and 50 exchanges. The thing to be aware of is that it won't generate 8949 or Schedule D forms if you're in the US or any of those international tax reports and audit reports. You also won't be able to export to TurboTax. Realistically this package is for anyone that wants to try Koinly out. You'll probably have to opt for a paid plan if you want to automate that paperwork to file those taxes. There are three different pricing plans. First, you have the Hodler. That will set you back $49 and supports up to 100 transactions, unlimited wallets and exchanges. It also offers access to all Koinly's features except for priority support, custom reports and report or import assistance. Next up is the trader pack for $99 per year. Get that and you're good for up to 1000 transactions everything in the Hodler pack and priority support. Finally the top tier Oracle package gives you access to everything Koinly has to offer and support for up to 300 transactions. If you need extra transactions then you can do that by upgrading that plan further to get support for over 10,000 transactions. That upgrade will cost you $279 in total. What are the pros of Koinly? Well, if you're looking for full crypto tax support in over 20 countries then this is the solution for you. It's also got the widest exchange and wallet support of any crypto tax solution I've seen. Also it has some unique and really useful features like the smart transfer matching system to make sure you don't make that tax overpayment. On to the cons, it's certainly not the cheapest solution on the market. If you only have a few transactions this tax year, I suggest you look at the $10 plan at Bear.Tax. Also would be nice to see even more country support rolled out too. So, who is Koinly is for? Well, if your country is fully supported and you have more than a few dozen transactions over the current tax year, then I think you need look no further than Koinly. That completes the best crypto tax solutions on the market right now. To find out more about Koinly, please visit their website at https://koinly.io/ The truth is that tax is a hassle at the best of times and let's face it no one really wants to spend days hunched over a calculator and an excel sheet. You might have to fork out a few dollars to get one of those crypto tax solutions however I imagine most people will say countless hours or days by getting their hands on one.

Chapter 19 No trading formula

Humans with inherent emotions that make us susceptible to making certain mistakes. These mistakes can be increasingly costly when you place money into the mix. Even some of the best traders in the world can fall victim to these psychological mistakes. But what are these mistakes? Well, in the following chapters I will share with you exactly what they are. I will also give you some top tips in order to prevent you from falling into the trap. It's important to point out that these mistakes are relevant for trading any type of markets. This includes cryptocurrency, Forex stocks and commodities. It's also quite a comprehensive list that covers a number of trading errors from the well-known to the less well-known. So if you feel that any of them in particular don't apply to you feel free to jump to the next chapter. The first and most fundamental mistake that newer traders make is not having a plan. No trading formula or investment hypothesis no structure to formalize their trading in a consistent and well-thought-out manner. They treat trading like a roulette wheel at the casino. Throw a few hundred bucks on one trade after the other. Hope for the best and maybe you pick the right trade that turns profitable. Quite expectedly this strategy is not profitable. In fact it's unprofitable. You'll win some, you lose some but in the end the trading fees will build up. Most of the time that new traders jump into the market they're doing so in expectation of making money. They want to move to that stage from the get-go and would prefer to forego the few days required to formalize a plan. What do I mean by a plan? Well, defined goals around target returned and the timeframe in which you want to achieve them. How much are you willing to risk and is it well within your budget. Then once you've formalized you need to develop a trading strategy. This itself is a pretty large task but can pay dividends in the future. What sort of markets are you looking to trade? Are you going to focus more on technical analysis or fundamental? In each of these there are a host of separate decisions that need to be made; timeframe, indicators and metrics. So you should be doing your homework. If you treat the markets like the casino then you'll always lose to that house edge.

Chapter 20 Taking a loss – now what!

People hate taking a loss especially when they think that there's a conceivable chance they can recover from a loss. This fear of taking a loss often leads them to make sub-optimal decisions. This is true for trading as much as it is for anything. They avoid cutting a losing trade as they hope it could recover. Even if the trade has proven to be a bad one, the trader will keep it open on the off chance that he was right and the market will correct itself. This is a fool's errand that often leads to more losses. Momentum is a pretty powerful force in the financial markets and if a trade breaks from your hypothesis, cut it quickly. Take the minor loss and reassess your position after that. On a purely psychological level you can think more clearly about your analysis when you're not being swayed by a losing position. Has the market really shifted? Was there some news that changed the variables and inputs? Did the market breach some key technical levels? All important questions that need to be answered before you place your next trade. While we're on the topic of placing new trades there is only one mistake more destructive than not closing a losing trade. That is chasing it and adding to it. Doubling down on a bad trade is one of the quickest ways to get wrecked and deplete your capital. Gamblers do it often and the term is called “gamblers ruin” as we've established. If a trade is going against you, it's more likely to continue with the momentum. Therefore if you add to that trade you could be slowly digging a hole that many traders have disappeared down. Of course there is one simple way in which you can avoid all of these risks in time. That is by simply avoiding one of our next mistakes; failing to place stop losses.

Chapter 21 Why you must place Stop losses

Stop losses are automated orders that are placed at key levels above or below your entry point. Dependent on whether you're long or short. Their orders that will close a trade without any intervention and can help eliminate the risk of flawed psychological thinking. If a trade goes against you and you don't adjust your stops, they'll be closed and will stop your losses. Another very important reason for stop losses is of course that they will still be executed even when you're not monitoring your trades. This is especially true of overnight markets like Crypto in Forex. We have to sleep and won't always be there to monitor our trades. There are numerous strategies when it comes to placing these stops as well as a large array of stock types that you can set. For example you can set stops at define technical levels. Or you can set them a few percentage points away from your entry level. You could also set a trailing stop that will remain a few percentage points away from your trade. It will automatically adjust if your trade moves into profit. Whatever stops you're going to be placing it should be done in tandem with your broader trading strategy. If you are scalping, then they should be very tight stops. If you're monitoring longer term trends then it can be placed just above a key capitulation point. So set a stop and let it ride. If you hit it there will be a loss but one that you mentally budgeted for and are willing to accept.

Chapter 22 Trading markets and Overtrading

The next mistake and this one is another classic rookie error; trading too many markets. Some of the best traders in the world are specialists. They know the ins and outs of a particular market and they focus on that almost exclusively. Essentially they own their domain. They know which markets they're most profitable in and which they are not. Some of the less experienced and newer traders on the market tend to want to trade a number of different markets. They want to be a jack of all trades. They'll jump into cryptocurrency and then trade Forex on the side all the while trying to experiment with stocks. Even if they're only trading one asset class having positions in too many different assets can be detrimental. A single trader can only pay a certain amount of attention and focus to a market. The moment you start splitting that attention onto other markets, you're hampering your performance in both. There is a very good reason as to while you'll want to focus in on only a few assets. You know exactly how it will react to important news. You learnt the relationship it has with key market variables. You get a bearing for all its quirks and features. There's also a precedent for this in some of the most profitable hedge funds and banks around the world. If you look at their trading floors, most traders will own a particular market. There will be a trader who specialises in gold options. Another in oil futures and a third in euro swaps. Those who are most skilled at a particular craft can provide so much more to an economy than those who try to perform 15 different tasks. So use the same principles when trading. Find a market that you'd like to trade and make it your own. Learn its ins and outs. Study the historical charts and understand its particular features. You could either do this when you're formulating your initial trading plan, or you can progress towards your ideal markets when you initially start trading. Of course that this does not mean you shouldn't trade more than one market. It means you should just be more discerning in the markets that you trade and put most of your attention on those you know you have a realistic chance of crushing. The next trading mistake I'll talk about is a slight variation of this and it is called Overtrading. Many people seem to think that trading returns are somehow correlated to trading activity. Then the amount of trades you push out could have some sort of an impact on your profitability. This is a fallacy and more often than not the opposite is true. You have those trading fees that

are charged on every trade that you make. The more trades that you make the more that these can rack up. Often the most valuable time spent those are the biggest ROI is when you're doing your research. When you're studying your charts and formulating your trading parameters. Actually executing the trade should only be a minor use of your time. After it is live you should be monitoring your open positions and adjusting them when your analysis warrants it. What is considered overtrading? Well, there's no real hard and fast rule. It really depends what kind of trader you are. Day traders will tend to trade more than those who have a longer-term perspective. Scalpers will trade even more than day traders. Sometimes if there isn't an attractive opportunity you don't have to trade at all for the day. Basically you should never feel compelled to trade even when there are no opportunities. There are no opportunities because analysis has not found a reasonable chance of profit. If you just trade for the sake of it then you're likely to confirm as much. So keep those itchy fingers away from the execute orders.

Chapter 23 Analysis Paralysis

On to the next mistake and this one is one more for the technical analysts out there. Using too many indicators. Those charts that some experts draw up with so many indicators and trend lines that it looks like a Christmas tree. The term is called analysis paralysis, and this is exactly what using too many indicators will do to your trading. This can cloud your judgment and overcomplicates your trading. Moreover, many of these indicators could contradict each other. You could have a great opportunity on the MACD and the RSI is at a reasonable level. But, the stochastic oscillator contradicts that. You throw on the money flow indicator and your trading analysis turns to mush. The same can be said for time frame analysis. If you're looking at moving averages from a plethora of different time frames, it could throw off your current analysis. For longer-term analysis the 200, 100 and 50 day timeframes are used. For shorter term trends you could examine the 10 or 20 day moving average. However there is no need to plot excessive moving average charts onto your graphs. So try to be on the side of simplicity for your analysis. Just because it looks overly complicated, does not mean it's better. You can easily spot that golden signal in the noise with a well-defined, yet limited set of indicators and charting tools. The next mistake is another really big one that people tend to make not only when it comes to trading but any sort of investments as well. You should never trade with more money than you can afford to lose. It's only practical. Apart from being highly irresponsible, it's also illogical. When you invest with most of your free capital you tend to be emotionally invested. The implications of losing funds become so dire that you can't help in it interfering with your analysis. You miss trades that you should have taken and you chase losses that you most definitely should not be chasing. So it's just sub-optimal from every perspective. You need to have money management strategy like you have a trading strategy. You have to carefully carve out a trading budget that you're comfortable staking. You should also be completely comfortable losing this stake, should the worst happen. If that happens you may cool off from trading for a month or two but you'll still have money in the bank. A roof over your head and food on the table.

Chapter 24 Leverage

So you have a budget set aside for trading but you now also need to be responsible with how you manage your risk. Another really common mistake I see traders making is using way too much leverage. Leverage is a double-edged sword. It can enhance your gains but it can also chop you down to size. Placing trades with limited margin down means that one unforeseen swing in the market could wipe out your trading account. This is particularly relevant in the cryptocurrency markets where you're trading incredibly volatile assets. Bitcoin has many mood swings and a negative move can leave you with less than half your money. Leverage to that and the losses are even more severe. Moreover, there's no reason whatsoever for you to max out your leverage. Just because you can trade with 100 times your capital, does not mean you should. You can be just as successful in the long run using leverage of even less than 20 times. So a well-thought-out money management strategy overlaid with a carefully crafted risk management strategy is the most effective way to stay in the game even in the bad times.

Chapter 25 Bad Broker Advice

The next mistake and this is one that most make before they've even placed a trade. Choosing the wrong exchange or broker can be a pretty big mistake but it's entirely avoidable. It's essential that you do proper research before you start using a particular exchange. These guys aren't the counterparty to your trade and they determine your trading environment. It's also worth pointing out that the broker and exchange space is littered with scams and bucket shop operators. Either they're out to rip you off or are so incompetent that your trading experience their leaves a sour taste in the mouth. So then what should you be looking for? Well there are a number of things but here is just a quick summary. Reasonable fees; it directly impacts on your profitability. Secure fund storage; you want your funds to be safe. Do they use segregated Fiat accounts in cold storage for their crypto asset coverage? You want to have some selection. Platform functionality; does it have all the technical tools you require? Is it intuitive and bug free? Execution effectiveness; can it place trades quickly with limited slippage? Are there regular system outages? Reputation; if they've been bad, you can be pretty sure other traders will have complained. Are there warnings and advisories out there? What are other traders saying? While some of these can be found out through just a bit of digging, most others can be discovered by trying the exchange or broker out. Create a test account, use demo funds, work your way up to the first deposit and even then start small. Once you've found an exchange that suits your trading style and ticks most of your boxes, then that's one less hassle to worry about.

Chapter 26 Choosing the wrong Exchange

The next mistake on my list is close to choosing the wrong exchange and that is following bad advice. We've all seen them on Twitter, Instagram and even on YouTube so called trading experts with their rented Lamborghinis and fake cash traders who advertise their lucrative trading returns as the reason as to why they can boar. The sad thing is that 95% of these wonder kids are nothing but effective marketers. People who could not really trade to make money so they're trying to sell their “incredibly successful trading services”. This could be in the form of paid telegram groups signals education packages or other money-making tips. Some of these guys make a killing selling these so much so that they can afford the lifestyle that makes newbies think they're great traders. It's a vicious cycle. There are so many free resources online. Everything that you could possibly want is at your fingertips. It just requires a bit of digging here or there. There are lots of successful traders and not a single one is successful because of the secret advice from an online guru has shared. Who are some of these false prophets? Well, I'm sure that you can spot them if you just use the simple rules of thumb just mentioned earlier. Most of these mistakes that I've mentioned are in relation to avoiding losses. But in order to be a successful trader you also have to effectively secure your gains. This brings me on to the final of the few mistakes traders tend to make. Never be scared to take a profit. If your trade has proven successful and you're comfortably in the money, then bagging those gains could be well worth it in the long run. Also traders tend to fall into the psychological fallacy that a trade that was successful will continue to be successful. They want to “ride their gains”. The problem is that this is more of a gambling tactic and it's equivalent to chasing losses. You're making decisions that are based on your gut rather than your brain. Gut feel trading is not the most reliable strategy for the long run. By all means, if you are analysis points to even better returns then keep the trade open. But do place some stops above your entry so that you can lock in those gains. It's also best practice to place some take profit stops at key levels or a certain percentage away from the entry. Blank the case with stop losses; this can remove the emotional component and will also ensure execution if you're away from your PC. Moving on let's assume that you've been placing a number of successful trades and things are going well.

Chapter 27 Overconfidence

The final yet most overlooked mistake is called overconfidence. Overconfidence and cockiness can work for certain fields and careers but it most definitely won't work when trading. When you start getting complacent about your trading price you start to get lacks in your analysis, you don't critically analyse your trades anymore and forget some of the key strategies that you employed to secure that profitable position. Arrogant traders also tend to take on more leverage, trade markets they don't know too well or worse yet, invest more than they really should. This is not a mistake that only inexperienced traders make. Some of the best traders in the world have yield to their own hubris. All examples of some really professional traders who thought they were invincible and in the end were proven not to be. So a healthy dose of humility pays huge dividends for long term trading gains. These trading mistakes you just can't afford to make. I hope these examples will help you avoid potential landmines that could blow up your trading returns. But truth be told much more is required if you want to be a consistently profitable trader. It's an iterative process that requires a hell of a lot of research and analysis. It takes time to formulate your trading plans and find the right markets and products to trade. Not only that, but learning the ins and outs of said markets can only really be done after months of actually trading them. There are no get-rich-quick trading schemes, but if you stay the course and keep your focus you will eventually start seeing the returns.

Chapter 28 Market Activity & Initial Research

When it comes to cryptocurrency there is arguably nothing more important than doing your own research. This is easier said than done. Who has the time to really do their due diligence with any given crypto project. After all there is a lot of information out there and it can be hard to figure out what's real, what's fake and what's just straight up hope and peddling. However if you're serious about you cryptocurrency ambitions you are going to need to learn how to do your own research. Research will help you figure out which cryptocurrencies to buy and which ones to stay away from. It will make it easier to figure out when to buy and when to sell those cryptocurrencies and it will even help you educate your friends and family about this magic internet money. And if you do enough research you might even find yourself working full time in the cryptocurrency space. In the following chapters I am going to teach you the art of doing your own cryptocurrency research and I will also reveal the research strategy i personally use. As we all know, the crypto market never sleeps and this means that sometimes you can't be waiting for someone to cover your favourite cryptocurrencies. At the end of 2020 we're at the start of a bull market and many people will have a lot of questions about a lot of different cryptos that you might not be able get as quickly as you wanted to. So this leaves you with only one option and that's to learn how to do your own research. The first step in doing your own cryptocurrency research is figuring out whether the crypto you're interested in, is economically active. I can't tell you the number of times that I've come across a promising cryptocurrency project only to check its market activity and see that the coin has been dead for months or even years. As such when you hear about a promising cryptocurrency that peaks your interest, the first thing you need to do is go to a website like Coinmarketcap or CoinGecko to see if it's alive. In most cases Coinmarketcap and CoinGecko will be how you find out about that cryptocurrency to begin with. If this is the case, be sure to check the training volume and price action you're seeing is genuine. Not only should that token be listed on at least one reputable exchange, but the trading volume on that exchange should also be significant. If it isn't, you could find yourself paying a premium since the order books may not be as deep. If the crypto you're looking at is an ERC20 token that's being traded almost exclusively on a decks like Uniswap, be sure to proceed with caution as Dex-s do not exactly have any listing criteria or requirements. This certainly does

not write off a project but it is something to keep in mind going forward. Also keep in mind that the price of a cryptocurrency and even its recent price action, is not a good enough reason for you to abandon ship with few exceptions. Once you've established the crypto you fancy has an economic pulse, it's time to get a sense of what it is and how it works. When it comes to wrapping your head around a new cryptocurrency YouTube is definitely a good place to start the problem is that you're probably going to find yourself skipping through videos of people reading off of website home pages and doing very poor technical analysis. That's why you should also pay a visit to Messari, Binance Research and an ICO tracking site like ICO Drops. When you use these resources, be sure to take notes and write down any questions you might have. You aren't trying to get answers yet, you're just trying to get a primer. I've mentioned Messari before as being a powerful tool you can use to analyse cryptocurrencies. In this case however what you're looking for on Messari is the profile section of the cryptocurrency you're interested in. Here you'll often find a thoroughly comprehensive breakdown, including the history of the cryptocurrency, incredibly detailed tokenomics and token allocations, and even a timeline of the project's past and future development and funding milestones. Be sure to write down the names of any key individuals involved in the project, namely the founder and CEO, assuming they're not the same person. You're going to need this later. In contrast to Messari, Binance Research often takes a more technical approach to analyzing any given token. This is useful in understanding the core components of the cryptocurrency you're interested in and how they work. The great thing about Messari and Binance Research is that because they're big players in the space, there is a degree of professionalism that's expected from them. In other words, they basically have to do a good job and get everything right or else fans of the cryptocurrencies they're writing about, will launch an attack and they could even see some more severe retaliation from the crypto project itself. The only issue is that the information on Messari and Binance Research is usually a bit outdated. You can't really blame them considering writing hot off the press crypto content isn't exactly their main thing. This is why you shouldn't take anything written by a third party as the ”be-all” and “end-all” of your research even if that source is reputable. ICO tracking sites like ICO Drops are sort of like time machines in that they often source old images and documentation that's no longer available on the website of the cryptocurrency you're investigating. This

makes it easy to spot whether a cryptocurrency project has changed its course, or if it's simply trying to bury the past. Unfortunately the total amount of money raised that's reported by ICO Drops and similar sites is not always accurate and tends to include any funds that were raised in private funding rounds or across multiple ICOs held by the project. As such you should always check and see if they provided any images that can give you a better breakdown of how money was raised and where tokens were allocated. Remember that Messari does a good job of tracking this so you can compare and contrast Messari’s data with what's on ICO Drops to clarify exactly how a given crypto project raised its capital. What you're looking for here is a token allocation that doesn't make you want to run for the hills. Specifically, you want to make sure that most of the tokens that have been issued or will be issued are in the hands of the community and not in the pockets of the people who founded the project. This is because they could potentially sell those tokens when the price starts to rise, which would prevent the coin from going as high as it otherwise could not. This is not a deal breaker, but could be if you checking a cryptocurrency's tokenomics on Messari. Assuming that everything seems to look good on that front, it's time to look at the source.

Chapter 29 Researching Technical Elements

Now that you have a good grasp of the new cryptocurrency you're interested in, you'll need to look at the source. Since you remembered to write down the names of the key individuals involved in the project, your next task will be to find the most recent interviews they've done that are up on YouTube. I recommend arranging them in chronological order before watching them. I found that watching interviews with key members of cryptocurrency project offer a treasure of information that you won't find anywhere else. Moreover, these interviews often go a long way towards helping me wrap my head around any technical elements of a project that I could struggle to understand by just reading their documentation. Chances are the things you hear during these interviews will answer most of the questions you might have had about the cryptocurrency when you read about it on Messari and Binance Research. Watching the brains behind a project in action will also give you a sense of whether you're dealing with the next best thing or with fool's gold. Also check their LinkedIn profiles to see if their credentials have any merit. Google or Microsoft doesn't mean anything if they worked there for a few months and then were fired for being drunk on the job. Finally try and see if you can find the YouTube channel of the cryptocurrency you're researching. If you're lucky you'll find short videos which explain the core components of the project in plain English. This leaves two more steps to your research and that's to fact check everything you've learned so far and figuring out what's in store for this crypto.

Chapter 30 Double-check the Source

How many times have you gone to the website of a cryptocurrency you're researching, only to feel overwhelmed by the information being offered. It's a big part of why most people just read the home page and the about section and call it a day. Unfortunately, most of the information on a given cryptocurrencies website tends to be platitude upon platitude about banking the unbanked or some other noble cause they claim to champion. To be blunt most of the content on a cryptocurrency's website is useless and isn't going to help you figure out if the project is worth your attention. And, you're going to waste a lot of time poking around through their site if you don't know what you're looking for. But since you remembered to write down the key components of how this crypto works and any questions you might have about it, your next mission is to go through and check that everything you learned still applies and solve any mysteries that might have arisen since you started your research. Most of this can easily be done by digging through the cryptocurrency's dedicated documentation. If you're lucky, you'll have a friendly search bar where you can just throw in key terms like tokenomics, inflation, ICO, consensus mechanisms, mining, staking and any other topics that you feel you still need clarification on. Otherwise, you'll have to search through the documents manually. Since cryptocurrency documentation is usually geared towards developers, many of the pages you pull out will contain some lines of computer code. This might seem intimidating, but more often than not you'll find that a simple explanation of what's going on is put at or near the beginning of the page in layman's terms. If you're still having trouble finding answers about tokenomics, try and dig up the white paper find the tokenomics section and see if this provides any additional insight. If it doesn't, try and find a blockchain explorer for that cryptocurrency. If it's an ERC20 token, I recommend using Etherscan by visiting https://etherscan.io/

Here, you can quickly check who the largest token holders are and you can even see the token distribution in a pie chart. Be on the lookout for any wallets that are holding a substantial amount of the token and remember that the largest wallets you see will sometimes be smart contracts used for things like staking. If your cryptocurrency of choice isn't an ERC20 token, hopefully the blockchain explorer for it will also let you see the rich list of token holders. If not consider that a red flag.

Chapter 31 Checking Upgrades and Roadmap

Now that you've an understanding of the cryptocurrency, the last thing you need to do is see if there are any important updates to the project that might be coming or have already happened. For the last part of your cryptocurrency research you are going to need three things; a roadmap, a blog and the news. And, in this order because usually what you see in the news about a cryptocurrency, is normally just a summary of what's been written on their blog. Note that these news articles can come in handy if the blog post they reference is too lengthy or complicated to digest. About the roadmap; from my experience, cryptocurrency roadmaps tend to be vague and do not usually provide too much information. You'll probably come to find that watching interviews with founders and CEOs will provide much more information about the future of a project than its roadmap. If you're lucky you'll find a roadmap that contains realistic goals that can be achieved before the project runs out of funding or gets wrecked by its competition. If you're unlucky, you'll get no roadmap at all and if the interviews you've watched don't give you a sense that the project is going to be around for very long you might be looking at a short-term investment. The future isn't all that matters though. You need to make sure that a project has delivered what it has promised so far. This is where the blog comes in. If you're having trouble finding a blog on a cryptocurrency's website, chances are you'll find it on their medium page. Sometimes you have to go as far as their github to see their progress and that's when you should really ask yourself if the project is walking on thin ice. Skimming through the headlines of a cryptocurrency project's blog is usually more than enough to get a sense of whether it's been true to its word and where it's headed. It's a good idea to actually read any updates you see that are significant, such as those relating to changes in tokenomics, or any big partnership announcements. Finally, open cryptocurrency news sites like cointelegraph, coindesk and decrypt and search to see whether what your promising project is up to has made the headlines. If you don't find anything, don't take that as a bad sign. As with the mainstream media the crypto media has its own way of doing things and it doesn't always shed light on the topics that need to be seen. By this point, you should have all the information you need to make a good judgment on whether a cryptocurrency is worth it or not. If you don't, then you're probably dealing with a crypto project that you need

to be very careful with or even stay away from. This could also mean that you'll have to go back and look closer at the resources you used in your research. Doing your own cryptocurrency research can be a lot of work but ask yourself this; are a few hours of research worth making for a 100x return or more on your investment? Yes, they are.

Personally, I do my cryptocurrency research by first visiting Coinmarketcap or CoinGecko to see if the token's being actively traded, preferably on reputable exchanges. If it's dead it isn't worth to look at it. Next, I go to YouTube and see what other people have been saying about the project. I take down a few notes if they mention anything noteworthy. Next I check out Messari and Binance Research to get a better sense of what the project is and how it works. I take down some more notes write down a few questions and write down the names of the founders. I then check ICO Drops to see how much money the project managed to raise and how the tokens were allocated. I use the images they've referenced along with Messari to double check that the details listed there are correct. Third, I go back to YouTube and watch almost every recent interview with the project's CEO or founder. More often than not, what they say answers many of the questions I'd written down in the second step. They also tend to clarify any confusing components of the tech that went over my head. I also checked to see if the cryptocurrency has a YouTube channel that offers additional insights and explanations. Assuming what I heard didn't turn me off I start the fourth step of digging through the project's documentation. I look for any additional details relating to the cryptocurrencies tech, tokenomics, consensus mechanisms, staking rewards, mining requirements and any other core components that I've learned about so far. Finally I search through their roadmap and blog to see if they've been making the progress they've promised so far and whether they can realistically deploy what they claim they'll be serving. Then I see if their activity has made the headlines in the crypto space. If not, this may present an opportunity to be ahead of the curve. Either that or it means that i just wasted a few hours of my time. I make this judgment based on the research I've done and to be honest I don't always get it right. In any case, I reckon this is a bulletproof strategy to doing effective cryptocurrency research. To me, it's the perfect blend of watching, reading and repetition that ensures that what I've learned, sticks around long after and helps me doing my next research to be carries out even faster. It's easy to forget that cryptocurrency is a very new field that's still very much in its infancy. This means if you can

get good at doing your own crypto research, you will become one of the few people who actually knows what's going on when the retail FOMO starts to hit during this bull market. The end result is not only that you'll make better investment decisions but you might just find yourself being offered opportunities beyond your dreams.

Chapter 32 Understanding Crypto Market Cycles

Imagine that we are at the end of 2021, Bitcoin has just hit its all-time high and is showing no signs of slowing down. Some altcoins have 10xed or you happen to be holding a substantial amount of one or more of these altcoins. The destination is clear; the moon. Is clearly in sight and now that you're so close to it, you start to realize that you never took the time to seriously think about the most important question in cryptocurrency investing. When should I sell? Perhaps you fly past the moon and you panic as you find yourself watch in shock as all your gains get burned up of the FUD. Well, in the following chapters I will focus on a few metrics you can use to help you plan your own ultimate altcoin exit strategy, regardless of what altcoin you're holding. To build a bulletproof exit strategy it is crucial to first understand the asset we're dealing with. This understanding starts with putting everything into context. The world economy consists of multiple financial markets such as housing markets, foreign exchange markets, stock markets and thousands of others. Almost all these markets follow some kind of visible cycle. It can be a one year cycle, a four-year cycle, or even a 12-year cycle. In some cases these longer cycles contain even smaller cycles that last a few months or even a few weeks. These cycles can also change over time. Usually becoming longer as a given market matures. The cryptocurrency market is very young and that makes it very volatile. This is simply because nobody knows for sure what the actual value of the market is. Older and more established investors hold much of the wealth in financial markets worldwide. These investors are generally more conservative and less prone to taking risks with their investments. Especially when it comes to new markets which consist of technologies they don't understand. This was actually the reason why Mastercard pulled out of Facebook's Libra project. CEO AJ Bangor said “when you don't understand how money gets made it gets made in ways you don't like”. In contrast, younger investors are a bit more tech savvy. We know how Bitcoin works as well as many of the promising altcoins in the space. We're also more prone to taking risks and many of us have serious “hope addictions” when it comes to our favourite altcoins. Not only that, but cryptocurrency markets are not restricted to suit and tie traders. All you need to participate is an internet connection and that means a lot of inexperienced investors. This makes the cryptocurrency market even more volatile and irrational on a day-to-day basis. Despite all the daily chaos in the crypto

market, when you step back you can see a pretty clear market cycle. This cycle seems to last around four years and consists of a two to three year bull market, followed by a one to two year bear market depending on how you draw your indicators. The cryptocurrency market cycle seems to be caused by the Bitcoin halving. The Bitcoin block rewards for miners are cut in half every four years. Assuming demand stays the same, the sudden decrease in supply eventually leads to a spike in Bitcoin's price. Since most altcoins are highly correlated to Bitcoin, they also see a massive swing to the upside around that time. This explosion in value, makes it to the media which brings even more money from both experienced and inexperienced investors into cryptocurrency markets. The most recent halving took place in May of 2020, leading many to believe that we are on the heels of another big move in the crypto market. Some would say we are already in it. In contrast to the two previous cycles, there is more smart money from financial institutions and experienced retail investors in the crypto space than ever before. This is in part due to governmental regulators around the world who have started doing their homework and realize that there is much more to cryptocurrency than Twitter hacks or ransomware attacks. And, the cryptocurrency market currently consists of anywhere between 7600 to over 8200 coins and tokens. The total market cap of all these assets combined currently stands at around 562 billion dollars. To view an up to date Global chart for the total Cryptocurrency market capitalization, please visit:

https://coinmarketcap.com/charts/

Bitcoin takes the largest share of this with a market cap of around 356 billion dollars as of end of 2020. As such, the cryptocurrency market is quite small compared to other financial markets and markets for similar assets such as gold. For context, the foreign exchange market is worth roughly 6.6 trillion dollars. While the market cap of gold currently stands around 9 trillion dollars. Many have interpreted this contrast in markets to be proof that the cryptocurrency market still has a lot of room to grow.

Chapter 33 Dynamics between Bitcoin and altcoins

Now that we have a solid grasp of the cryptocurrency market it's time to take a closer look at the individual assets inside of it. As we all know Bitcoin is the first cryptocurrency and remains the largest and most popular by a wide margin. Every other cryptocurrency is consequently referred to as an altcoin. While this dichotomy is debatable it is a very important one to keep in mind nonetheless and here's why. The likelihood that the market cap of any altcoin will be larger than Bitcoins anytime soon is very low even during the next Bull Run. This is for one simple reason Bitcoin is where most of the smart money from institutional investors and experienced retail investors is going. You won't see huge companies buying the dips on altcoins like any time soon. Even Ethereum is having a hard time getting into the hands of serious investors. This seems to be partially due to the upcoming release of Ethereum 2.0, which has some large investors like Greyscale which do hold Ethereum, calling ETH 2.0 a material risk to investment. Compared to altcoins, Bitcoin is much less volatile and its volatility has been gradually decreasing over the years. What's more is that its price action has a significant influence on altcoins. When Bitcoin goes up altcoins go up. If Bitcoin goes up too quickly, many altcoins tend to see losses in the short term, especially those with a smaller market cap. Why? Well, because most of the money invested in altcoins is coming from crypto rocketeers who are looking for the quickest path to the moon. When we see Bitcoin taking off many of us ditch our altcoins and rush to the Bitcoin spaceship. And when Bitcoin loses steam and the price drops everything comes crashing down to earth. Altcoins tend to see their best gains when Bitcoin is gradually increasing in price or when it's trading sideway. This is partly because opportunistic investors get bored with the price action from Bitcoin and the other large altcoins and start inching closer and closer to the deeper and more chaotic waters of what lies beyond the top 10 or 20 altcoins. These dynamics between Bitcoin and altcoins are absolutely critical to understand because your ultimate altcoin exit strategy starts with the awareness that it will be heavily influenced by what Bitcoin is doing. The upper limit of where your altcoin could go is effectively set by Bitcoin's own market cap. While it's true that Bitcoin's market cap will likely continue to grow as the bull market marches on, planning to sell your XRP when it hits 1000 dollars is not a realistic exit strategy because that would

give XRP a market cap of over 50 trillion dollars. That's more than double the size of the entire US economy.

Chapter 34 Comprehending Tokenomics

Now you have a sense of how Bitcoin's price action seems to influence altcoins and have also hopefully come to the realization that the market cap of your favourite coin is probably not going to be larger than Bitcoins anytime soon, the next step is to factor in the tokenomics. If the US dollar was a cryptocurrency, it would have some of the worst tokenomics in the crypto space. It has an inflation rate of around three percent per year. It has no supply cap and can be created at will by a centralized authority. Most of its circulating supply is held by a very small amount of people. This makes it a very poor choice as a long-term investment and this has prompted one of the largest collective exit plans in financial history called cryptocurrency. It is quite amazing that almost every single crypto coin has its own unique tokenomics. What's more, is that the open source nature of many of the blockchains these cryptocurrencies are built on, make it easy for anyone to see exactly what is going on with their favorite tokens. This sort of transparency is refreshing as it's quite rare in legacy finance. However, it also shows us that the cryptocurrency space is not immune to the same sort of corruption and greed found in our current monetary systems. I've lost count of the number of times I've come across a crypto project that was promising in every way only to be let down by its tokenomics. So many cryptocurrencies have solid development teams with functioning products and platforms that have clearly defined and valuable use cases, even boast partnerships with numerous internationally recognized institutions. Then you open the block explorer and it's worse than going through you could ever wish for. We are going to cover the key tokenomic factors which you need to keep in mind when it comes to planning your ultimate altcoin exit strategy. The first is token allocation. Every cryptocurrency has its own unique token allocation and a select few had no token allocation. Instead, a genesis block was mined by one or more parties at the beginning without any sort of special token distribution. This is known as a fair launch and is unfortunately quite rare in the crypto space. Most cryptocurrencies we see today had something called a pre-mine. This usually involves allocating a fixed amount of the initial or total supply of a token to select parties or causes. Some of these tokens go to the founders, others go to early investors of the project and usually the largest chunks go towards the ICO and mining or staking rewards

for those who will participate in that cryptocurrency's ecosystem. When you look at the altcoin you're holding, take note of how these tokens have been allocated in the crypto project's ICO documentation. Then check to see if those tokens have actually been allocated in the way that was initially outlined. You can do this by using a block explorer, which you can usually find on your altcoins website. If the altcoin you have is an ERC20 token you can use Etherscan to easily check what's going on behind the scenes. Your mission is to figure out which wallets are holding a large number of tokens and whether those could be suddenly sold if the price were to increase significantly. It's safe to assume that tokens allocated to opportunistic venture capitalist firms or angel investors will be some of the first to go. If you see a single wallet holding more than 10 of a token's total supply, you might want to reconsider your altcoin pick. That said, some cryptocurrency projects have vesting schedules for allocated tokens. These mean that those tokens given to investors or founders will not be available right away, but over time or just at a later date. If you see a vesting schedule like that you might want to consider selling your tokens sooner rather than later. The second thing to watch out for when it comes to tokenomics is inflation and total supply. Inflation is not necessarily an issue, so long as it's low and so long as you aren't planning on waiting to sell when you retire. It's also important to mention that inflation is used by many projects to incentivize network participation. This means you can sometimes avoid this inflation by staking or delegating your tokens if you plan on holding onto your tokens for some time. However, the sort of aggressive token inflation that's used to pay liquidity providers in many D5 protocols will probably cause several issues in the first place. With these tokens, it is best to follow the wise words of finance's creator: “do not buy it, earn it”. The DiFi token might just be the best example of how important the supply metrics of a token is, in regard to its price. DiFi is one of the few cryptocurrencies that have a higher price tag than Bitcoin. The simple explanation for this is that the demand for the token is exponentially greater than its maximum supply of thirty thousand. Who wouldn't want to own a token that gives them a say in how one of the best D5 protocols is run. This small supply is also why DiFi's market cap is just 400 million USD. Not only that, but all DiFi tokens are in play. There are no additional DiFi tokens waiting to be mined or minted. DiFi also had a pretty fair launch with no pre-mine. All tokens were earned by liquidity providers on yearn finance. These characteristics have led some to label DiFi the Bitcoin of D5. In summary,

check that your altcoin had a fair launch or at least an equitable pre-mine with a vesting schedule that doesn't make you run for the hills. Make sure that inflation isn't too high and see if there are ways you can mitigate against it, until you decide to sell. And be sure to take note of the circulating supply, compared to the maximum supply assuming there is a maximum supply. Otherwise, you might find your tokens suddenly losing value as additional coins start to flood the market to drown out demand.

Chapter 35 Technical Indicators

There is one last thing you need to take into account to finish planning your ultimate altcoin exit strategy and it's what the technicals are saying. An exit strategy relies on technical indicators. While technical indicators can be very useful, their utility declines in the absence of other critical factors, such as the ones we've outlined in the previous chapters so far. What's more, is that technical analysis can suggest different trends, depending on the time frames you're using and the way you decide to draw your trend lines. That said there are two technical indicators you need to pay attention to when it comes to deciding when to pull out. The first is Bitcoin dominance. Bitcoin dominance is how much of a cryptocurrency's total market cap is accounted for by Bitcoin. Currently it's 63.4% and seems to have been declining steadily since the past year when it was around 68%. During the last crypto bull run in 2017 and 2018 Bitcoin dominance fell to just 37%. This is important because the large amount of money moving into altcoins is part of why many alts saw their all-time highs during that period. Assuming this downward trend in Bitcoin dominance continues, we may just see another sudden drop in Bitcoin dominance in the next year or two. If this happens, it will once again bring a flood of money into the altcoin space and take many alts to new all-time highs. Historically, big drops in Bitcoin dominance have lasted around one to two weeks, meaning you would have plenty of time to exit during that window if that's part of your ultimate altcoin exit strategy. The second technical indicator to keep in mind is your altcoins value against Bitcoin. Most of us are focused on the dollar value of our favorite altcoin and prefer to trade against a stable coin like USDT. While this may make it easier to keep track of our portfolios, it is the value of your altcoin in satoshi's that gives you the best indication of whether your cryptocurrency is rising in value, relative to other assets in the crypto space. Let me give you a simple narrative we're all familiar with. Suppose your favorite altcoin has been rising in dollar value. You're feeling good and you start to feel the keys of that Lamborghini materializing in your hands. Then you click over to the rankings and see that other altcoins are making even more impressive gains and your favourite altcoin is barely keeping up. Maybe even lagging behind. Well, if you'd taken a closer look at the Bitcoin pairing of your altcoin you would have noticed that even though your altcoin was rising in dollar value, it was actually losing

value in satoshis. Whereas some of those other altcoins had been gaining value in satoshis. Again, the time frame you use to analyse this trend might influence whether it's going to the upside or the downside. If you're lucky you'll see a clear trend you can spot on a short to medium term time frame that will tell you whether your altcoin is valuable in terms of real money or in terms of fiat. Keeping a close eye on Bitcoin dominance and your altcoins trend against Bitcoin will help you figure out when is the best time to sell.

Chapter 36 Exit Strategy

Now that we've covered all the metrics you need to build your very own ultimate altcoin exit strategy, it's time to run a model. Suppose there is a cryptocurrency called XYZ coin. XYZ coin currently has a market cap of 100 million dollars meaning it just barely cracks the top 100. Like other altcoins it is highly correlated to Bitcoin which currently has a market cap of 300 billion dollars. I really love XYZ coin but i know it's not going to be bigger than Bitcoin. I also have doubts that it'd be bigger than Ethereum which currently has a market cap of 50 billion dollars. As such, if it were to go suddenly parabolic now I know it would probably not be likely to pull off more than 50 times move in price. Since that would make it as big as Ethereum. XYZ coin has an initial supply of 50 million and a maximum supply of 100 million. Each token is currently worth 2 dollars and the inflation rate is one million coins per year, meaning I can wait up to 50 years before XYZ coin enters uncharted territory. 100 of XYZ coin's initial supply is currently on the market and 20 percent of this supply has been reserved for my friend who was an angel investor of the project. But he's not able to touch his tokens until January the 1st 2023. So I know it will probably be a good idea to sell before then because I know my friend is all about fiat currency and will dump as soon as he can. Now let's fast forward. It's the end of 2022 and XYZ coin has already 10xed in price over the last few months. Meaning that each token is worth $20 and the market cap is just over 1 billion because of inflation. Bitcoin's market cap is just under 1 trillion and Ethereum's is over 500 billion even though ETH 2.0 still hasn't been released. Bitcoin dominance saw a sharp drop one week ago and money is flooding into altcoins, meaning I have no more than a week before that trend starts reversing. XYZ coins pairing with Bitcoin could be better but if I look carefully, I can see a slight uptrend on the one day time frame and XYZ coin has jumped to almost $30 within a minute. I think that a 20x from my initial entry is possible but reason that a lot of traders are going to sell XYZ coin at the psychologically comfortable level of 50 dollars. To play it safe i set a limit order to sell my XYZ coin at $34. I go to bed then I wake up and see that XYZ coin has hit a high of over $65 while I slept, but now is only $18. It would have been nice to sell the top but that's an impossible task. Price looks bearish now and all indicators suggest we're headed for a huge correction across the board. Should I sell?

Well I better do then stay on holding because my friend will dump within a week and the price will get even lower. As you see, all it takes is a bit of research, a bit of strategy (and lots of luck).

Chapter 37 Crypto Exchanges: Coinbase Pro

There are a lot of crypto exchanges out there. Gone are the days when you were strapped for choice. Today, the choice is overwhelming. This is not only a challenge for those new to crypto. But it also means those who are currently using an exchange constantly have to wonder if they really do have the best deal. Do not worry, because in the following chapters I am going to give you exactly what you need to know about the best exchanges on the market right now. I will cover both pros and cons and compare them side by side. This is to help you assess your options and pick the right crypto exchange for you. I'm sure that many of you are like me and some of your friends make fun of you when those crypto markets are in the toilet. However when those markets are blasting off then I certainly get asked the question; what's the best crypto exchange? Every single time I turn around and just tell them that they're asking me the wrong question. The better one to ask is; what's the best crypto exchange for me? After all we all prioritize different things. So there really is no one-size-fits-all answer here. With that in mind I want to be straight up and just say the following exchange picks are in no particular order. Still first I will start with Coinbase Pro which is an advanced trading platform, operated by Coinbase. So who are these Coinbase people? Well, they were one of the first companies to enter the crypto exchange game back in 2013. The company is based in San Francisco and has 35 million users that have traded 220 billion dollars in volume. Another fact is that Coinbase's most recent round of funding for 300 million dollars valued the company at 8 billion. This means it’s a pretty serious crypto exchange. So that brings me on to a key question; who can use Coinbase Pro? Well the good news is that Coinbase is accepted in over 100 countries. So the chances are that you'll be able to trade on Coinbase Pro. This also includes the US in any state other than Hawaii. Signing up to Coinbase Pro is pretty straightforward, but the thing to know is that you need to create a regular Coinbase account first and then log into Coinbase Pro. Your login and password for Pro are exactly the same as your basic Coinbase account. Once you log into Coinbase Pro you'll see a trading panel. Here, you can place a market or limit order and stops. I know that may sound complicated and daunting to crypto newcomers but I can promise you that it is quite straightforward. Another feature offered on this exchange would be leveraged trading up to three times. I would not recommend using leverage unless you know what you're doing and the

comfortable trading spot markets. For many newbies this is a very fast way to get to a place called “wrecked”. Not a place that I recommend to anyone to visit. When it comes to deposit methods it's a little all over the shop at Coinbase and dependent on which country you're based in. But major supported payment options include bank transfer, PayPal debit and credit card. Now let’s look at the fees. It can be tempting not to pay too much attention to these, but they do add up and can seriously eat into your long-term profitability. There are two main fees here; deposit and withdrawal fees and trading fees. Let's look at deposits first. The thing to know is that ACH and swift deposits are completely free. USD wires are charged at $10 and SEPA Euro deposits incur just 15 cents in fees. Withdrawals are free for ACH 25 for USD wires 15 cents for super transfers and $1 for swift. The good news for people wanting to withdraw crypto off the exchange is that this is entirely free. If you are like most people and are trading less than 10 000 per month, then you'll be paying 0.5% in trading fees. That scales down the more volume you do. The next thing to talk about is the range of cryptocurrencies available for trading on Coinbase Pro. Some people might use Coinbase Pro to just buy Bitcoin and send it over to another crypto exchange to buy more altcoins but right now about 40 different cryptos are available for trading. That's not too bad at all. All of us hope to never have to use customer support, but it is something worth considering when choosing an exchange. After all it's annoying if you have a problem and you're left hanging for ages. At Coinbase Pro you can submit a support ticket through their form and they'll get back to you over email. But being honest, personally had my patients stretched to breaking point by Coinbase support. They just seem to ignore me for days so just be aware of that if you opt for Coinbase Pro and pray you never need to reach that customer support. Coinbase Pro does offer phone support 6 am and 6 pm but here's the bad news. These support agents cannot help with any account specific queries like order statuses, specific transactions or your account history. Every customer support query I've ever made has been linked to one of these things. So this type of support might as well not be there if you ask me. The next thing to discuss would be security. Coinbase Pro holds 98 of user funds offline. Those private keys are then split with redundancy, encrypted and copied to super secure USB devices and paper backups. These are then popped in safe deposit boxes scattered throughout the World. So if you want to keep your funds on an exchange, Coinbase is pretty secure. Coinbase Pro

also has FDIC insurance for US dollar accounts. This is the same insurance banks use to protect customers. What that means is that us dollar balances below a quarter of a million dollars are insured by the US government. Good news if you're a US citizen and are holding us dollars on Coinbase. In terms of securing your account, Coinbase Pro has a host of security features like two-factor authentication. One major drawback that I need to tell you about is the frequent exchange outages at times of high market volatility. That can be annoying if there is a massive market move which you can't take advantage of. Finally, Coinbase Pro does offer IOS and android mobile apps for those that want to trade on the go. If crypto trading bots are something that you're interested in then the good news is that most major third-party bot software supports Coinbase Pro. Now you know the ins and outs of Coinbase Pro, you might ask; who is it for? Well, honestly Coinbase Pro is probably the easiest one to use but you should know that you'll be paying some of the highest exchange fees out there for that privilege and dealing with less than stellar customer support. If you're new to crypto and are wanting an easy way to get into crypto using fiat, then Coinbase Pro is certainly worth considering. But there are probably better options out there for more experienced crypto traders. To get started with Coinbase, please visit https://www.coinbase.com/

Once you have registered, you can also be able to log on to Coinbase Pro on the following link: https://pro.coinbase.com/

Chapter 38 Crypto Exchanges: Uniswap

Uniswap is a decentralized market making exchange. It's essentially an open source dap built on Ethereum that enables you to swap eth for any ERC20 token in a truly decentralized way. All that is combined with a simple and easy to use interface that also connects to popular web 3.0 wallets like Metamask. How does Uniswap differ from centralized alternatives like Coinbase Pro? Well, on Uniswap there is no company holding your funds and instead, you're always in control of your own crypto assets. In other words, it is non-custodial. I know that may not sound like a big deal but try telling that to the poor souls who had their crypto controlled by the likes MTgox or cryptopia. The lesson to learn from these centralized exchange disasters is that things can go bad in a very big way if you trust the wrong company with your crypto. Indeed that's the key reason why so many people in the crypto space support decentralized exchanges. Here's something that a ton of people don't know. In September 2020 Uniswap actually reported more trading volume than Coinbase. Gone are the days when DEX-s were a plaything of crypto geeks. The upshot of Uniswap's decentralized nature is that there are no country restrictions to speak of. In terms of unique features, liquidity pools are what makes Uniswap decentralized and are the mechanism through which you can actually earn trading fees with Uniswap. These are basically pools of tokens which sit in smart contracts. Another feature that privacy adds value is that there is no KYC to speak of on Uniswap. So if you value that, then this is the exchange for you. Because Uniswap is non-custodial, that means there are no such things as deposit or withdrawal fees. Instead, you'll pay Ethereum gas fees to send those tokens to the protocol and a 0.3 liquidity provider fee to swap them. I do need to give you a brief warning about these Ethereum gas fees. If the network is super congested, then these can cost you a lot! Indeed, in early September 2020 a straightforward ETH to Defi swap on Uniswap cost $55 in gas fees. Since then, these fees have fallen to more reasonable levels but just keep an eye on those fees before you make a swap. Another thing to note is that Uniswap is solely an ERC20 crypto to crypto exchange. That means to use it, you'll need to have at least some Ethereum or ERC20 tokens already. There are no fiat deposits or withdrawals here. In terms of supported cryptocurrencies if you want to get your hands on an ERC20 token then chances are it's listed on Uniswap. There is literally

hundreds of cryptos but just be aware that you won't be able to get your hands on any cryptocurrencies outside of the Ethereum ecosystem here. Next, let’s look at the Customer support. As Uniswap is a DEX, things work a little differently here. The best way to get help here is by bumbling into the Uniswap discord group and asking your question in the support chat there. For those of you that are trading whilst out and about, Uniswap doesn't really have a dedicated mobile app. However you can launch the app in your mobile browser and connect to a mobile wallet. The Uniswap UI is well optimized. Seeing that Uniswap is non-custodial you might not think there are any security concerns. But the key risk here is the same as any other D5 project and that would be smart contract bugs. I've not heard of anything on that front, but just be aware of that. So who is Uniswap for? Well, in my opinion it's the perfect exchange for anyone who is reasonably experienced in crypto and wants to keep control of their private keys and not entrust their funds to a centralized exchange. Privacy hawks will also love the lack of KYC. But some might find the lack of support for crypto outside of the Ethereum ecosystem limiting and gas fees can sometimes make the exchange excessively expensive to use. To get started with Uniswap, go to https://uniswap.org/

Chapter 39 Crypto Exchanges: Binance

My next exchange pick is called Binance. The first thing to note is that there are several versions of the Binance exchange. You have the likes of Binance Singapore, Binance Uganda, Binance US etc. The thing to know is that these are different exchanges from Binance.com. Which you can think of as Binance's global exchange. Very simply, Binance is the biggest exchange in the world and processes around 2 billion in daily volume. So who can use Binance.com? Well if you're based in the US, Uganda or Singapore, you'll have to use the version of the exchange for your respective countries. Aside from that, the only countries blocked are those that fall under US sanctions. When it comes to exchange features, on Binance you get access to the most extensive crypto spot market in the cryptoverse. A suite of advanced trading tools such as the ability to trade on margin and an over-the-counter service to get you better pricing without slippage. Then, there are a host of advanced derivative products. These enable you to dabble in futures markets with up to 125 times leverage and to long or short tokens with up to three times leverage. Next you have crypto finance services like Binance earn, which allows you to earn bank interest rates on your crypto. The Binance crypto card gives you cashback of up to eight%. You also have access to flexible collateralized crypto loans. Then there are exclusive initial exchange offerings that you can take part in on the Binance launch pad. So there are plenty of features to Binance. When it comes to deposit methods all crypto deposits are free. Withdrawal fees are variable and dependent on the crypto or fiat currency you're getting off the exchange. Binance also supports some of the lowest fees for any exchange too. Remember I mentioned before that you would get rinsed for 0.5% in trading fees on Coinbase Pro? Well, Binance kicks things off with a 0.1% maker and taker fee. Pay that fee with BMB coin and you'll get another 25 off. Trade a ton, and you'll get further fee discounts too. Binance also supports a range of deposit options for many different currencies. Yet they have recently activated Visa and Mastercard deposits in addition to methods like bank transfers. Bank card fees for Euros and GBP attract a fee of 1.8%, whereas UK faster payments and SEPA bank deposits are entirely free. That brings me on to supported cryptos. In short, literally almost any crypto worth looking at is listed here. In terms of customer support, Binance has you covered 24/7 with an online ticket system.

Those Binance customer support agents will then get back to you over email. I have never had to wait more than 24 hours to hear back from them. When it comes to apps, Binance has gone the extra mile with an excellent mobile app for android and ios and a desktop app for mac os, windows and Linux. So if you like apps, then Binance has you covered. Touching on security, Binance does use best practices when it comes to cold storage, multi-signature wallets, tiered access and enhanced cyber security detection systems. But the exchange did get hacked in 2019 for 7000 Bitcoin which was about 2% of all its Bitcoin holdings. What we can learn from this, is that Binance holds about 98% of its users funds in cold storage. Pretty much the same as Coinbase Pro. With all that being said users impacted by the hack were all reimbursed by Binance. Needless to say, Binance is supported by every third-party trading bot worth considering. So with all that in mind, who is Binance for? Well, honestly Binance is for anyone who isn't shy of dabbling in altcoins.

To check out Binance, please visit https://www.binance.com

Chapter 40 Crypto Exchanges: FTX

The next exchange I will introduce is called FTX and this one is for advanced traders out there. FTX is an exchange founded in May 2019 and is registered in Antigua and Barbuda. Their offices are based in Hong Kong. The exchange has also raised 8 million dollars in external funding and was raised by Alameda research, a quantitative trading firm that trades up to one billion dollars a day and manages over 100 million dollars in assets. Who were some of those investors? Well one was Binance who announced a strategic investment in FTX earlier in 2020. The key takeaway here is that FTX is a serious crypto exchange with some serious backers. When it comes to blocking countries, FTX doesn't accept residents of the United States, Cuba, Iran, Syria, North Korea or Antigua and Barbuda. So if you're living in any of those places then you are out of luck here. In terms of features, you first have the standard spot markets with dozens of different cryptocurrencies to choose from. Then you have the widest range of perpetual futures markets that I've seen. Then you have a host of three-time short and long leveraged tokens, volatility tokens and some really interesting indexes. You can buy a basket of coins on FTX using their index or maybe you just want to get exposure to defy easily by getting their defy index. If you're an options trader, FTX has also got you covered with some Bitcoin options as well. The exchange also offers an OTC portal so those whales can get those trades done with minimal slippage. A great deal if you need to get large block trades done. So FTX has a whole host of features geared towards the more advanced traders out there. But, what are the fees? Well taker fees start at just 0.07 and scale down from there according to trade volume. FTX is the cheapest exchange. When it comes to deposits and withdrawals for crypto assets FTX has the best price possible; free. Though the thing to know here is that if your deposit or withdrawal amount exceeds your trade volume on the exchange, then you might be charged a 0.1% fee. So you probably don't want to deposit here if you're not going to trade much. When it comes to fiat deposits credit cards and wire transfers would be the methods available to you. I need to be honest and warn you that if you're withdrawing fiat using FTX then you'll incur a $75 fee for withdrawals under $10,000. In terms of crypto support, FTX doesn't offer the widest range of cryptos for spot markets but it does offer the largest range of perpetual futures that I've come across and a ton of special

futures products like the coin index. So, if that's what you're looking for, then FTX is a great choice. In terms of the support, FTX has simple email support options. When it comes to security, FTX operates a cold storage protocol, so the majority of the funds are stored offline. For individual accounts, they also have two-factor authentication and you can whitelist IP addresses too. Finally, as FTX operates a leveraged exchange one of the major risks is volatility and that's why FTX operates an insurance fund. This insurance fund acts as a reserve in case liquidations of losing positions cannot be done fast enough. That insurance fund currently sits at about 2 million dollars and an additional 5 million FTT tokens. So, who is FTX for? Well, the exchange is for experienced traders looking to use those instruments like perpetual futures and leveraged tokens. If that's want you wish to trade, you won't find a better selection anywhere else. If you're interested in signing up to FTX, please visit https://ftx.com/en

Also, while I've explained about exchange security, I don't recommend anyone keep large coin holdings on a centralized exchange unless you're actively trading. No matter how secure an exchange might be, there is simply no substitute for a hardware wallet to give you that maximum security. It's an old saying but it's always been true: “not your keys, not your crypto”.

Chapter 41 Leveraged Trading Basics

Leverage trading is one of those highly controversial subjects. some view instruments like futures and swaps as directly responsible for the wild moves in the crypto markets. Some see them as a tool to actually hedge said price moves and timber volatility. Some people see them as a dangerous product that have wrecked many inexperienced traders. Others view them as an essential tool when used responsibly. So who's right? Well that's exactly what I will explore in the following chapters. I'll take a look at both arguments and break them down, separating fact from fiction. We'll also explore some of the more unsavoury practices in the space as well as some of my personal tips when it comes to using these instruments. Before I can take an in-depth look into the leveraged trading industry, we need a bit of an intro to it. So what is leverage trading? Well quite simply it's trading with more money than you have. To expand on that a bit more, it's entering positions on the market that are many multiples of what you're putting down as collateral. This collateral is more commonly called your margin and it usually measured as a percentage the amount that you can trade with. So for example if the margin is 20% of the position, it implies a leverage of five times. The margin of 10%, implies a leverage of 10 times. This means that your position is levered up by a certain factor. Gains and losses a magnified by the said factor. It's this quality of leverage trading that can either make it lucrative or deadly, depending on which side of the trade you are. Leveraged trading is quite broad and there are a number of different instruments that can give you leverage. You have Financial Futures, Swap Instruments, CFDs or Contracts for Difference or even pure Margin Borrowing to trade. There is another aspect to some of these leverage instruments and that is their ability to be used to short sell an asset. This basically means that you'll be able to make money from a fall in the price of said asset. That is a basic overview of what leverage instruments are, but in order to understand their role in the crypto markets, we have to take a brief look at their history in traditional finance. Futures instruments are almost as old as finance itself they were initially used centuries ago as a method for farmers to hedge the risk out of forward prices for commodities. They would sell their product into the future in order to secure a price for it when it came to market. Fast forward a few decades and these instruments became tradable products on large exchanges such as the CME or Chicago Mercantile Exchange. No longer were they just a product to

hedge the risk for farmers and buyers, but they became a method to speculate on the price of a commodity. Who just wants to speculate on soybeans and orange juice? Well, futures markets eventually rolled out to the currency markets in the early 1970s. Interest rate markets in 1975 and stock indexes in the 1980s. Eventually by mm you had futures instruments on single stocks as well. These were mostly traded by institutional investors on large regulators exchanges such as the CME and CBOE. Those traders would keep margin accounts at exchange members which required less than the notional size of the contract. These margin accounts pretty high and hence implied a leverage of only between three to five times. The fact that futures were not offered to retail traders is an important point though. There were indeed quite high risks that came with trading them. Losses could be multiples of the margin and retail investors were not considered well-versed enough to trade these financial products. Eventually these did make their way into the retail markets through the numerous online brokerage accounts offered to US traders. Futures and margin borrowing were no longer exclusively the purview of institutional investors. However leverage limits have remained between 5 to 20 times depending on the asset. Also it's worth noting that these brokers are heavily scrutinized by the likes of the US Securities and Exchange Commission and the CFTC.

Chapter 42 BitMEX & BTC Futures

Fast-forward to early 2013 when trading started picking up in a new and relatively unexplored market. That was of course the Bitcoin market and with it came the opportunity to offer exotic and uncheck leverage trading instruments. One of the first exchanges to offer leverage Bitcoin trading through futures was BitMEX. BitMEX is registered in the Seychelles and ran out of Hong Kong. This was one of the major Bitcoin futures exchanges for a number of years. They gave Bitcoin traders the opportunity to trade their perpetual futures instruments of up to 100 times. Given that the Bitcoin markets are largely anonymous and anyone could have created an account, anyone could have traded them and they did. From large-scale whales to small fishes, all hoping to cut their teeth in leveraged Bitcoin trading. The thing is that whales eat small fishes and so do exchanges too. BitMEX started generating a reputation as being a bit of a meat grinder for the small fry. An extremely efficient liquidation engine was pretty effective at cutting highly leveraged traders down to size. Without any oversight regulation or competition BitMEX literally controlled the Bitcoin futures market. There were also a number of rumors that they operated their own trading desk and used their users positions to their own advantage. Would be similar to playing poker with someone when they can see your cards. Traders still gathered to the exchange however via law of being able to make a hundred times your initial investment on a single trade was overwhelming. But not only were the cards stacked against these traders but they also had no clue what they were doing. Forums were flooded by cautionary tales of traders who got wrecked and speaking of wrecked, there was actually a Twitter bot that was started to track the size of the liquidations on the BitMEX exchange. I don't mean to scare you away from leverage trading, I just wanted to give you a bit of a background of it in the crypto markets. BitMEX has since restricted us accounts and they have a lot more competition. So they've had to defend their market share. There are a overabundance of futures exchanges that have opened up in multiple regions. Here is just a few of them; Deribit, bybit, FTX, Phemex, KuMEX and you also then have numerous spot crypto exchanges that have either offered their own futures products or enabled some form of leverage trading. These include Binance, Kraken Huobi DM and OKEX. Even Coinbase has enabled some margin trading functionality on

their platform although with lower leverage limits. Something else also happened back in 2017. The CME and CBOE both released their own regulated and Exchange listed Bitcoin futures. Demand for these products has steadily been increasing over the past three years. This was mainly driven by a surge in institutional interest in Bitcoin futures. So much so that other providers like Bakkt also listed their own physically settled Bitcoin futures, the first of its kind. So the point is that the Bitcoin futures and leveraged trading market has evolved quite a bit. Much like the spot Bitcoin markets themselves they're less Wild West more Wall Street. Less unregulated online casino, more sophisticated and regulated instruments. This is the general statement about the shape of the Bitcoin futures and leverage training market. At the end of the day it always comes down to the individual trader and how they use it. It's a tool that can either be used effectively in a risk managed way, or irresponsibly in a reckless and destructive manner.

Chapter 43 Leverage Trading Strategies

The first major responsible use case for futures instruments is actually as a mechanism to reduce your portfolio risk. Essentially, it's a method for market participants to hedge out the volatility of the underlying asset. Think about an asset manager that has a large physical Bitcoin portfolio. They may want to reduce the risk around a potentially volatile period. The having for example. They could then short the futures market and effectively eliminate that risk. Or, what about miners that are bringing new Bitcoin to the market. How do they secure that price for their product? Much like the farmers of yielding times they want a method in order to be able to sell the product at a predetermined price in the future. Not all those who are using futures are going to be hedging. There are many that are trading them as they are more cost effective method than trading the physical coin itself. If you're a Bitcoin trader you want to be able to maximize your return for a given price move. Leverage helps you do that. Those who use leverage responsibly are also generally more experienced with trading in general. They would have made money in the spot market but preferred to enhance those gains. They also always play stop losses and know exactly how to avoid particular trading mistakes. Finally, they also know how much leverage is enough. This is a clear distinction between them and beginners. They know that you don't really need more than ten times leverage to be able to trade effectively and responsibly for the long term. This is in stark contrast to those that are using futures instruments and leverage trading irresponsibly. Sadly it's these people who the exchanges make most of their money off of. So what is this irresponsible behavior of which I speak? Well people should not be trading with leverage if they don't know how to trade spot. If you are not going to make a profit trading with no leverage, you sure you aren’t going to with leverage. You should also not be using leverage if you don't know how it works or how to manage it. Most tend to forget that it's a double-edged sword that can also chop you down to size if not controlled on the downside. For example many still do not trade with stop losses which is silly. But perhaps the biggest mistake that these traders make is the amount of leverage that they take on. Exchanges will flash a headline number of 100 times leverage and those new of the game, will go and open up an order. With that exposure this sets them up perfectly as food for exchange liquidation engines. Even

minute moves in the price of Bitcoin can have large impacts on the PNL of your position. Let's also not forget that Bitcoin is one of the most volatile markets in the world. It's also no coincidence that the leverage factors and margin requirements on regulated exchanges or retail brokers is much lower. This could either be down to regulations or whether high leverage levels are even demanded. For example over at Bakkt the initial margin requirement is about 37% which implies a leverage of only about 2.7 times. On the CME, margin could be as high as almost 50 which implies a leverage of only about two times. This is indeed quite low for many professional traders but it shows you how little leverage is really needed for a product to be appealing to retail investors. The guys who manage billions of dollars are perfectly fine using this leverage. So why do you need 50 or even 100 times leverage. The main reason that anyone will want to trade with such high leverage ratios is because of the same reason that they throw some numbers down on a roulette wheel. It's not trading, it's gambling. This gambling is great business for the exchanges.

Chapter 44 How Exchanges make money

At the end of the day an exchange is just a centralized trading engine that matches buyers and sellers of futures contracts. They will charge Commission on all of the trades that they match. Apart from facilitating the exchange they also make sure that the trading pool is kept solvent. They have to make sure that in the event of extreme market moves, those that are close to depleting their margin will have their position closed. This is to protect what is called bankruptcy in the position. To do this exchanges operate liquidation engines. These are basically mechanisms that will close out trades at the liquidation level. This liquidation level is usually above or below the bankruptcy level, depending on whether it is long or short. Having this buffer in place ensures that the exchange is able to close your position long before it threatens the solvency of the pool. When they run their liquidation engine it executes trades which mean trading fees for the exchange. Simply, higher leverage means more liquidations, which means more trades, which means more trading fees for the exchange. Not only is the exchange earning bank on that liquidation but they're also using any excess funds after the liquidation is executed to fund their insurance pool. What is that? Well, it's a reserve fund that will be used in order to prevent situations of socialized losses. Basically, those situations in which the other side of the trade are harmed, those insurance funds can grow to become immense. For example over at BitMEX the fund stands at over 37,000 Bitcoin. All funded from the margin of wrecked margin traders. The larger the leverage, the larger the gap and more likely a liquidation and the more chance of your margin being chucked into the insurance fund. High leverage also has a broader impact on the spot Bitcoin market. As more traders use excessive leverage, it leads to unwarranted situations ripe for mass market liquidations. All one needs is a small price adjustment and a cascade of liquidations whipsaws the spot Bitcoin market. Only those who could see a mass liquidation event coming; whales for example will profit from this. Everyone else is left holding the back. So on every level high leverage that above ten times is suboptimal for everyone apart from the exchange.

Chapter 45 How to use leverage responsibly

Firstly, you should consider if you even want to do it. Have you traded in the spot market before and have you developed a trading strategy? This could be a fundamental one based on price action or a more technical one that is shaped by the charts. Do you have a money management strategy? Essentially you should know exactly how much you're willing to trade. This should be viewed as a completely separate component from your huddled portfolio. It should also be funds that you should be comfortably able to lose without breaking the bank. You should then decide on what exchange you want to trade. You have no shortage of different options anymore. The chances are that if you're already using any large crypto exchange, then they could have a margin trading or futures feature. Exactly what exchanges you use will depend on the functionality you need as well as the coins that you want to trade. Bybid for example have the most efficient trading engine and a highly functional trading interface. It's one of those exchanges that offers high leverage but you should never go above fifteen times. You can find out more about bybit by visiting their website at https://www.bybit.com/en-US/

There are many people who don't want to use a centralized leverage exchange like bybit and that's understandable. Another exchange that I have used in the space is called dYdX. They are basically a decentralized margin trading platform that uses smart contract technology to facilitate leveraged trading. The max leverage over here is five times on the margin trading platform and ten times on their perpetual contracts, which is good enough for most. Caution; liquidity is pretty limited and you don't have nearly as much functionality or efficiency as a centralized exchange. This is just the nature of defy currently. We hope that the launch of Etherium 2.0 and other scaling solutions could help to supercharge decentralized trading platforms. In the end it's a really touchy subject. Some view them as instruments that have been shielded to inexperienced traders to benefit whales and exchanges. But one can't paint the entire billion dollar Bitcoin futures market with the same brush. Leverage trading when used responsibly can optimize portfolios and actually reduce risk. It's not about the instrument itself but how it's being used. Irresponsible trading will wreck people whether they trade Bitcoin a hundred times, go all-in on some altcoin or sink all their ETH into a defy lending pool. Risks should be assessed and managed. Some leveraged

exchanges make it all too easy for beginners to get Rekt’. They offer the same instruments to those traders with years of experience as they do with those who just started trading a few days ago. But that's why it's imperative that those margin trading on these exchanges understand exactly what they're doing. They need to know just why high leverage is suboptimal and dangerous. If we have less people trading these instruments as a casino and more people using them in a responsible manner, we'll have less people with unpleasant experiences. Moreover, if we have fewer people leveraging the markets then we won't have those price swings that make the markets feel like a roller coaster.

BOOK 7

BITCOIN AND CRYPTOCURRENCY TRADING

FOR BEGINNERS

TRADING BOTS, CANDLESTICK PATTERS

AND

TRADING PSYCHOLOGY

BORIS WEISER

Chapter 1 dYdX: Margin Trading Features

Cryptocurrencies are all about decentralization. Individual control of our assets that no one can restrict or seize. Yet it's always puzzled me why seemingly decentralized assets are overwhelmingly being traded on centralized exchanges. Nowhere is this more prevalent than on the crypto derivative and margin exchanges. People think that there are no real decentralized alternatives and even if there are, they require a PhD to operate. Well that was until dYdX opened their protocol. In the following chapters I'm going to share with you everything you need to know about dYdX. I'll also

take you through the process of trading lending and borrowing on dYdX, as well as comparing it to some other apps. So what exactly is dYdX? Well, simply put it's a noncustodial decentralized crypto exchange or DEX. However unlike most other Dex's, here you can lend borrow and trade on margin. It's an open source trading protocol that was built on the Ethereum protocol and is powered by smart contracts. Given that it's non-custodial it means that no one else but you are in control of your private keys. Trading is done by connecting your Ethereum wallets to the exchange. No KYC, no limits, no questions. It was started back in 2017 and they raised over ten million dollars in seed funding from some well-known VC funds. It went live in May of 2019 and has grown considerably since then. There is currently just under 19 million dollars locked into the protocol and it's the 8th most used app. There has also been over 200 million dollars that has been traded on the protocol. So much growth for dYdX? Well, this comes down not only to its functionality but also its relative simplicity. An ideal mix for adoption from the broader crypto community. Let's take a look at some of these features starting with their primary MO; margin trading. Trading on the margin means increasing the size of your exposure to an asset through leverage. At the large centralized exchanges such as BitMEX the exchanges will loan you a position in an underlying crypto for only a small deposit, the margin. With a leverage position your gains and losses are magnified by the leverage factor. At a decentralized exchange, they will monitor your positions and if they deteriorate to a certain level then you will be liquidated. This is all done by the internal liquidation engine that these exchanges run. You can't see how these engines work and you don't know all the parameters that are used in those algorithms. At dYdX on the other hand the protocol is open-source. Fully auditable smart contracts adjust leverage ratios, free up margin and if need be, liquidate positions. You can see exactly how the protocol works in a fully transparent manner. Leverage at dYdX goes up to a maximum of five times or an equivalent margin position of 20%. You might be thinking that you can get up to 100 times over on BitMEX! Well, yes you can but do you really need 100 times leverage to be profitable? Let's not forget that leverage is a double-edged sword and you can lose just as quickly as you can gain. Is the benefit of trading with so much leverage worth the risk of trading against your preferred instrument? Five times leverage on a decentralized exchange is pretty good for most traders that know what they're doing. Also with lower leverage you have less risk of liquidation. Another really good feature that

you have a dYdX is that you have two types of margin mechanisms you have isolated and then you have cross margin. Isolated margin is the mechanism that you're most likely to be quite familiar with. It's where you will isolate a particular amount of your funds as part of a trade with a specific leverage level. If there is a liquidation, the losses will be capped to your isolated position. But cross margin is something different. This utilizes all assets that you have in your account. It takes into account your combined position in your account when it is determining leverage and limits. There are a number of reasons as to why you may want to cross margin your trades. When it comes to trading pairs you have ETH-DAI, ETH-USDC and DAI-USDC. You can trade the difference between a centralized and decentralized stable coin. While leveraged trading is one of the selling points of dYdX, don't forget that's also a standard Dex. You can trade the above spot assets in the spot market.

Chapter 2 dYdX: Lending & Borrowing

The next feature that I want to share with you on dYdX is their lending feature. When you're lending your crypto out on dYdX, it's being lent out to other users on the platform and you are earning an interest on that deposit. This interest is earned on a continuous basis and is sent straight to your wallet. This is also relatively risk-free lending because the dYdX protocol ensures that the borrower's are over collateralized. What do I mean by that? Well, they have a collateralize a shin ratio that requires more crypto collateral than they have borrowed. This means that the market was to move quickly, there are enough funds to pay back the lenders. Another really great thing about dYdX and defy lending gaps like it is that there are no restrictions on the deposits. You can withdraw the funds lent whenever you like. The concept of a term deposit is alien in the crypto space. Given that this is a decentralized app there is no entity or intermediary that's controlling your lending. It's all managed through the use of transparent and decentralized smart contracts. This makes it quite different from other crypto lending platforms such as BlockFi or Nexo. The final primary feature of dYdX is the ability to borrow. Part of the reason that dYdX can operate a leverage Dex is because of the global lending pools facilitated by the protocol. These pools apply to a particular asset and are all operated by smart contracts. Supply and demand in these lending pools will determine what is called the utilization ratio. This is basically just the amount of funds that are utilized in the lending pool. So borrowed amount divided by supplied amount. This will have a direct impact on the interest rates that are being charged or earned. It's pretty clever. The same happens in traditional financial markets. Interest rates are seen as the cost of capital and they move according to how many people want to borrow a fixed portion of capital, versus those who want to supply it. That aside, borrowing on dYdX can be done up to a minimum collateralization ratio of 125%. Anything below this level and you cannot borrow any more crypto. Once that crypto hits 115%, your trade will be liquidated. This is in order to keep the trading pool solvent and keep the lenders that we talked about earlier hole. Those who are liquidated will have to pay a liquidation fee of 5%. This is done in order to make short borrowers keep their accounts well collateralized and firmly above the liquidation level.

Chapter 3 dYdX: Margin Trading Step-by-step

Now you have a reasonable overview of the main features of the dYdX platform, but how can you use it? Well, it's actually pretty simple. So simple in fact, that you can even be forgiven for forgetting that it's a Dex. From the homepage of dYdX, you can select what you want to do trading, borrowing or lending. For me I'll discuss trading, so if you click on that, the main dYdX user interface it's pretty well laid out and looks much like your typical centralized cryptocurrency exchange. Here, you have your order forms, your order books, the buy/sell walls, charts open orders and positions. It's actually neat that they've included this trading view chart as this will allow some of you more technical traders to run your TA. You can also switch the chart here to view the market depth. In order to trade on dYdX or any decks for that matter, you have to connect your wallet to the dap. You can choose from any wallet here you can connect your ledger if you want but I will give you an example with Metamask. Once you wallet is connected, you'll need to approve the transaction on your device and you're ready to go. Like with any exchange, you'll need to deposit assets in your account. Given that you also have that lending component, you should note that the moment you deposit funds at dYdX, it will be placed into the lending pool and you will start earning interest. Give it some time for the network to process the transaction. Once it's fully confirmed and deposited into your account it will be reflected on your balance. Now you're ready to trade. Given that we're going to trade on margin, you have to select that one. Going to go long on ETH-USDC pair, you can choose the position size as well as the leverage. As mentioned your max is 5 but you can set a custom leverage limit if you want. When it comes to the Advanced Options, you can set your max slippage. This is basically the maximum amount that you will allow the price to fall and would still be happy executing the trade. If the price slips past this max slippage point, then the order will be cancelled. Regards to the expiry time point, dYdX trades are not perpetual. You can think of them more as regular futures that have expiry times. So once you reach expiry, the position will be automatically closed out. Once you're fully comfortable with the parameters and then you can place the order and it will go into the books. You'll be able to monitor your trade in the positions tab as well as your PNL. You also should keep an eye on that collateralization ratio. If you slip below the liquidation point, then you'll have your position closed and lose that liquidation fee. That’s it. This is the margin trading feature.

Chapter 4 dYdX: Spot Trading & Lending Step-by-step

Spot trading is much like the other standard Dex-s that you have seen. You will technically be swapping one crypto for another. You also have a lot more order functionality than you do on the margin trade. These include placing market orders, limits as well as stop orders. You can also select how long you'd like the order to remain open. It's time forced. So there is a bit more customization options around your orders here. Do note that if you have any leverage trades open, trading in the spot market will impact on your margin and in turn, collateralization ratio. So keep an eye on that. When it comes to lending on dYdX it's pretty simple. As mentioned, the moment that you deposit crypto onto the exchange, it will start earning interest. You can see those interest rates over in your balances tab at the top of the platform. Here you will have both the lend and the borrow rate on the various assets. You should also note that dYdX will take a 5% cut of all interest payments in order to fund an insurance pool to protect the protocol. This is already reflected in the rate. These rates are annual percentage rates but have paid continuously into your wallet. To complete this walkthrough, let's take a quick look at the borrowing feature. Here, at the top is the tab to borrow funds on dYdX. It's a pretty straightforward layout. On the left you have all your asset balances. Here you can repay outstanding balances and you can borrow new assets. Then in the center, you have all your outstanding borrows. Borrowing crypto is pretty simple. All you need to do is select the crypto that you want to borrow. Choose the amount you want to borrow as well as the crypto that you'll be depositing. For example if you want to borrow DAI and will be depositing ETH, you hit borrow DAI and confirm the transaction on your wallet. You will see the outstanding burrow show up in the center as well as all the interest rate that you'll be paying. That does it for the platform walkthrough so let's take a look at something I'm sure you want to know; the fees. Until recently it used to be free to trade on dYdX. You would sign a message to create an order in the book. When those orders were matched, dYdX submits a transaction to execute the match trades on chain. dYdX would have to pay the gas costs for this transaction. While this works smoothly with smaller trading volumes, as volume picked up this year so did gas costs. In February 2020 they had to fork out over at least $40,000 in gas fees in order to cover it. There was a change in March of this year

where they announced that they would start charging fees in order to cover this cost. The fees that are being introduced will follow a standard maker take a model. Essentially those who are making markets and providing liquidity will get a lower rate than those who are taking it off the book. In the case of dYdX, makers will have zero fees and takers will be charged a few percentage points. Do note that there is a different take a feat for those who are trading less than 0.5 ETH. This is only logical as gas fees on transactions for small orders are just as large of those of larger orders. If we were to compare these fees to some of the larger exchanges such as Binance, the taker fee on orders above 0.5 ETH is slightly lower. Whereas its higher with orders below 0.5. Still pretty impressive for a decentralized exchange. In terms of any other fees that you could have to pay on dYdX, you have that liquidation fee that I mentioned and then if you allow the trade to expire, it will have to be traded. This trade carries a 1% price spread. All in all these fees are reasonable and are the cost of maintaining a secure and highly functional defy protocol.

Chapter 5 dYdX: Trading BOTs

dYdX has built a pretty simple client and trading API that will allow you to build trading BOTS. Much like you can build BOTS that interact with the large centralized exchanges, you can develop them here to trade on chain at dYdX. Except, when trading a dYdX you can place instant non-custodial trades. There are also a number of other benefits that can come with building bots at dYdX. Not only can you programmatically partake in the margin trading, but you can also run a liquidation bot. What is that? Well at dYdX you can also participate in the liquidation of under collateralized positions. Doing so, earns you that 5% liquidation fee that I mentioned before. If you're running a bot 24/7, you can basically scan for these under collateralized accounts and take advantage of them when the moment arises. dYdX have even provided the code for an open source liquidation bot. One of the final few things I want to look at is the competing d5 project dYdX is up against and how they compare. There are a number of other projects ranking higher in value locked than dYdX. The top three are actually quite interesting called; maker, synthetics and compound. Maker is a decentralized autonomous organization or DAO, upon which the DAI stable coin is built. Since the issuance of DAI, it's become the most popular decentralized stable coin on the market. There was also recently an upgrade of the eco system to the multi collateral DAI. Basically this is also a lending protocol that has got a decentralized exchange feature as well. This is all done through the Oasis defy hub. While the lending and borrowing features are pretty straightforward the trading feature is left wanting. It's pretty basic and is way less advanced than dYdX’s. Just after maker is synthetics, this was another really exciting project. It's a decentralized trading protocol that allows crypto traders to take positions on synthetic crypto assets. It does not only have to be crypto but it can also include a number of traditional asset classes. You can also trade inverse assets which would be similar to shorting a pair. There is no doubt more trading optionality than dYdX, you don't have margin trading. I also find that the trading interface is pretty basic when compared to that of dYdX. Of course some people find it's simplistic which is a plus. Finally, you have compound finance. This is a lending protocol that has also been making waves recently. It also has a pretty sizable lending pool. Apart from the size of the lending pool you also have much more optionality when it comes to

lending and borrowing. Something that is pretty neat was the wrapped Bitcoin lending. This basically means that you can lend an ERC20 asset that tracks the price of Bitcoin. You can't trade on it like a Dex and you don't have margin trading optionality, so it won't really satisfy your needs there. I really like what the team is doing and they have built a pretty effective Dify dap. It's pretty easy to use for most crypto traders used to the large centralized exchanges. The simplicity does not come at the cost of reduced functionality. Lending, margin trading, borrowing and liquidation are all part of the dYdX package. The recent introduction of trading fees may disappoint some of the earlier traders on the protocol but it was always expected. Upgrades take time and developers got to eat. I would recommend giving dYdX a try if you haven't already. Of course be sure to manage your risk and never trade lend or borrow more than you can afford. If you are interested to sign up or want to look at the platform you can find it at https://dydx.exchange/

Chapter 6 Introduction to Trading Bots

When it comes to day trading crypto there are such an amazing opportunities out there. But there is one major problem. Crypto markets never sleep and most people need to catch sleep from time to time. That leads to many traders going to bed and waking up only to discover they missed out on a huge market move and an amazing trading opportunity. This isn't a problem for some traders. Why is that? Well, it's because some use crypto trading BOTS. In the following chapters I'll explain what crypto trading bots are. I will also go over the pros and cons of using them and compare the top trading BOTS side-by-side. So what are crypto trading bots? Well, they are computer programs that trade on your behalf with a given set of instructions or rule criteria to act on. So that might be something like buy X amount of Bitcoin if a certain price target is hit. Once that rule criteria is met, then the bots will automatically execute the trade you wanted. What this means is that in order to use a crypto trading bot, you will need to connect it to a crypto exchange account using something known as an API or application program interface. Basically that API gives your trading BOTS the ability to place trades programmatically at the exchange. The result is that you can execute trades in your sleep. You're essentially handing over access to your exchange account to a computer program. What happens if there is compromised code in the bot or the company that made the crypto BOTS turn out to be scammers? These are all very real concerns that you must be aware of. Are the machines going to take over your Binance account? Well not exactly. The good news is that you can set permissions for exchange API's. You can determine what particular API keys have the ability to do in your account. So for the crypto trading BOT, you can set the ability to only write orders buy or sell but not to initiate a withdrawal. Most likely a good idea. You can also limit IP addresses too. What that means is that any instructions must come from your own IP address which is a neat way to protect yourself against a scammy crypto trading bot. So now that you know what a trading bot is I want to go over the pros and cons of using them and give you some cold hard truths. One major Pro is that these BOTS enable you to trade 24/7 and execute trades in your sleep. That means you'll never miss out on the another trading opportunity ever again. Also trading BOTS help take the emotion out of trading. You are simply setting the rule criteria or instructions in the bot and

leaving those trades to execute if your criteria are met. That means you should be less susceptible to FOMO or panic selling. Another benefit of using bots is that they allow you to back test your trading strategy. What that means is that a bot can take that strategy you're using and apply it to all that historical crypto price data and tell you how successful it is. Finally trading bots simplify trading. But they are pretty expensive. Given that a crypto trading bot can access and simultaneously carry out multiple trades across multiple different exchanges you only need a laptop to be trading. Still not all is well when it comes to crypto trading BOTS. I'm going to have to be straight up on the cons. Many people seem to be under the illusion that trading BOTS are some form of magical money printing machine. Get one, switch it, on and you make money all day long. Sorry but that's not the case at all. With a bot you have to constantly tweak your trading strategy. That is work and it is certainly not a set and forget it money printer. Another con for crypto BOTS is that there are a bunch of scams out there. Even if you find a legitimate one some are so poorly coded that it's going to be impossible for you to execute a single profitable trade. Therefore you need to be really careful with crypto trading BOTS. If it sounds too good to be true then it probably is. I will list a few trading BOTS shortly, but if you choose to use a different trading BOTS that’s completely fine. It's always good to assess your options but if you see trading BOTS claiming to guarantee returns for low one-off pricing, please run for the hills. More than likely it's a scam. Another thing many people do not realize is that crypto BOTS need to be monitored. Do not expect to switch on a crypto trading bot and be laughing all the way to the bank. The market is cyclical. Trends come and go all the time. Basically a bot is not a substitute for being a smart trader. To use them, you will need to keep your funds on an exchange. There are a lot of highly reputable and secure exchanges out there but hacks do happen. With all that said, in the following chapters I will list some of the best and most well-known crypto trading bots.

Chapter 7 Trading Bots: TradeSanta

TradeSanta is cloud-based BOT and has a solid reputation with over 45,000 active users 14,000 active trading BOTS and 1.8 million completed trades. However I do want to give you a fair warning. It may take you a while to get used to some of the functionality. When it comes to features, TradeSanta offers a long bot template to use when you expect a crypto asset to rise in price, a short bot template when you think it will fall and a custom template which gives you the freedom to leverage the full functionality of the bot. In addition to all that TradeSanta offers you a excess of technical indicators to digest. These include things like Bollinger signals, trade filters and volume filters. Another neat feature that is great is the real-time tracking, which enables you to monitor the bots progress on-the-go with transparent analytics and telegram notifications. TradeSanta has also got an iOS and Android app. When it comes to exchanges, TradeSanta supports HitBTC, Binance, BitMEX, Houbi, OKEX, Bitfinex and BITtrex too. In terms of pricing, the good news is that TradeSanta offers a 5 day free trial. So you can jump in there and play around with the bot to see if it's worth your hard-earned money. After that you can use the free version which gives you access to just two bots and has a maximum monthly volume limit of $3,000. On top of all that, you'll get access to an unlimited number of trading pairs, all TradeSanta strategies, telegram notifications and general customer support. The basic plan gives you access to everything the minimum plan offers, while unlocking access to up to 49 BOTS and allowing you to run an unlimited amount of trade volume through the bot. That will set you back $14 a month. This is the plan I recommend for most people who choose to opt for TradeSanta. However you can upgrade to the hit BTC promo plan for another $7 per month. This gives you everything in the basic plan plus 0% trading fees on HitBTC. Some might say that's a valuable benefit but I'm not the biggest fan of HitBTC. The top pay plan on TradeSanta basically gives you access to everything the basic plan does, plus the 0% in trading fees on HitBTC and access to an unlimited number of bots. That will set you back to $70 per month. Honestly I doubt any of you will really need to shell out $70 a month. So what are the pros and cons of TradeSanta. Well you should certainly have this bot on your short list if you want lots of automated trading options and are looking for an intuitive interface and reliable security

measures. The bot is also well suited to beginners dipping their toes into the crypto bot waters. Needless to say, automating your crypto trading with such a tool is going to give you loads of time and there is a super active trading community, to meet like-minded traders too. Still, there are drawbacks. It lacks support for some of the major high liquidity exchanges like Kraken and KuCoin and doesn't support any decentralized exchanges. It's also not really suitable for taking advantage of arbitrage opportunities and is not open source. Who is TradeSanta for? Well, in my opinion this bot is ideal for any crypto day trader that's not interested in futures trading and envisions that they will take crypto bots seriously. It's also beginner friendly, so if you're new to the world of crypto bots then this is a great place to start. To learn more about TradeSanta, please visit their website at https://tradesanta.com/en

Chapter 8 Trading Bots: Shrimpy

Shrimpy is a social portfolio management tool and crypto trading platform that bursts onto the scene in 2018 and quickly gained a ton of popularity in the trading community. The value proposition was simple. Provide as many top-of-the-line trading tools for the lowest price possible. That's why they offer a good range of services for free. What's important to note is that Shrimpy is not designed for signals or indicators. So it's not the best tool for day traders. Instead it is a longer-term portfolio management tool which automates things like portfolio rebalancing, dollar cost averaging, and stop losses. That approach is perfect for anyone that wants to take a top-level view of their portfolio and wishes to automate the management of that. Unlike other trading bots that provide almost every possible indicator, signal and stat, Shrimpy eliminates that complexity by focusing only on core long-term trading strategies. That makes things super easy for beginners and this is also why Shrimpy is normally the first crypto trading bot I recommend to friends interested in this bots. Another important feature is their social portfolio management. This enables you to take a bit of a backseat when it comes to managing your funds and allows you to select other traders to manage your portfolio for you. You can also select the best traders on the platform and get a copy of their trading strategy without, copy trading them. That's a great learning tool and you should definitely check out. Also Shrimpy offers a pretty powerful back testing tool. So if you have that ultimate trading strategy that you want to put to the test, then you can do so right here. Right now Shrimpy doesn't have a mobile app. If that's important to you then you should certainly weigh up other options. The Shrimpy crypto trading bot is also supported on a ton of different exchanges such as KuCoin, Binance, Coinbase, GEMENI, OKEX, Bitfinex, Poloniex, BITtrex, BitMart and Huobi Global. What's the cost of all this? Well Shrimpie offers a pretty extensive free plan that allows you to link unlimited exchanges to monitor your portfolio performances, blacklist assets gives you access to an asset balance tracker and more. However if you want to automate that portfolio management back test those trading strategies or use Shrimpie social trading features, then you'll need to opt for a paid plan. That will set you back just $13 per month if you opt for the annual plan or $19 per month if you want to pay monthly. Additionally, Shrimpie does offer an enterprise plan too. So

what are the benefits and drawbacks of Shrimpie? Well they offer a lot of features entirely for free and the subscription fees are quite reasonable. If you are a crypto HODLer and want to automate things like portfolio rebalancing and dollar cost averaging, then Shrimpie is going to save you so much time. The social trading feature is also ideal for anyone that wants to leverage the knowledge of top crypto traders that do nothing but eat, sleep, trade and repeat. In terms of drawbacks ,Shrimpie is not open sourced so you're going to have to trust the thousands of people using it that the code is good. Also there's no mobile app which could be a deal breaker for some. Finally, Shrimpie does not provide the functionality that most active day traders will need. If that's you then there are certainly better options out there coming up in the following chapters. In my opinion Shrimpie is a top option for long term crypto holders who want to automate that portfolio management or want to copy trade some of the best traders in the space. To learn more about Shrimpie, please visit their website at https://www.shrimpy.io/

Chapter 9 Trading Bots: Gunbot

The next crypto bot on my list is called Gunbot. Gunbot also known as Gun-T. It's a pretty popular crypto bot that is compatible with Mac, Windows and Linux so you can run it on practically any computer. When it comes to features Gunbot comes with numerous inbuilt trading strategies that include the likes of step game, gain and ping pong. Another cool thing is that you can customize your trading strategies in Gunbot and the bot will execute those trades for you. When it comes to mobile support Gunbot is pretty well mobile optimized. Gunbot also supports a ton of top-tier exchanges like Coinbase Pro and margin trading on BITmex, Kraken and OKEX. What's the pricing for Gunbot? Well this one differs from the rest which have a subscription-based model. Instead Gunbot charges a one-time license fee. The starter pack is 0.02 Bitcoin. However you'll only be able to use Gunbot to trade on one supporters exchange and access free trading strategies. Gunbot standard offers access to all trading strategies, but you will still only be able to use the bot on one exchange. That will set you back 0.05 Bitcoin. Gunbot Pro is where things start really heating up in the pricing stakes it will set you back 0.075 Bitcoin but you will be able to use the bot on three exchanges and you'll get access to trading strategy back testing too. The bot also offers a wide range of add-ons and upgrades as well. In terms of pros and cons, I really like the variety of trading strategies on offer at Gunbot. It's also easy to use and supports exchanges like Coinbase Pro but the downside is that Gunbot feels relatively expensive with its one-off fee structure. Who is Gunbot for? Basically anyone who wants a beginner friendly crypto trading bot that intends to be trading crypto seriously for a long time. To learn more about Gunbot, please visit their website at https://www.gunbot.com/

Chapter 10 Trading Bots: Crypto Hopper

Next crypto bot on my list is called Crypto Hopper. Crypto Hopper provides expert trading tools without the need for coding skills. If you are into more advanced trading stuff like market making and exchange arbitrage, then this bot has you covered. The Crypto Hopper marketplace also boasts a plethora of trading templates, strategies and signals to choose from. These signals allow you to subscribe to professional analysts around the world and Crypto Hopper uses these signals to trade. But be warned that not everything in the marketplace is free. If you want to access your trading bot on the go, the good news is that there is an Android and iOS app. When it comes to crypto exchange support, Crypto Hopper integrates with KuCoin, Binance, Coinbase, OKEX, Bitfinex, Poloniex, BITtrex, HitBTC Kraken and Huobi Global. In terms of cost, Crypto Hopper offers a 7-day free trial. The basic pan will set you back 16 dollars per month and is ideal for more day traders. If you're into exchange arbitrage then you'll be paying $41 per month and the market making license is 83 dollars per month. What are the pros and cons of this bot? Well on the pro side it is easy to setup keenly priced. The marketplace is great and there is good coin and exchange support. If I was to have one gripe it would be that I cannot see who is behind the bot. Transparency goes a long way in crypto. Who can benefit from Crypto Hopper? Well honestly almost anyone that is interested in using a pro level crypto bot at a reasonable price. To learn more about Crypto Hopper, please visit their website at https://www.cryptohopper.com/

Chapter 11 Trading Bots: 3commas

My number one trading bot is called 3commas. What you need to know is that this is one of the most popular BOTS out there with over 140,000 users and 65 million dollars in trade volume every day. It has a super intuitive interface packed full of detailed analytics and a ton of functions. The bot also enables you to set stop loss and take profit targets and craft your own trading strategies. Personally I find 3commas smart trading functionality particularly useful. For example you might want to buy Ethereum with Bitcoin. But on some exchanges when you make an audit you need to decide if you want to set a take profit, or a stop loss. You cannot always set both and that's pretty inconvenient. But with 3commas that is something you can do as well as set trailing stop losses easily and quickly. That means, if the market jumps up 5% then the trailing stop loss raises your stop-loss by 5%. Some exchanges do allow you to set take profit levels and stop losses at the same time but if that trading pair you want to trade isn't there, then you don't have to pass up that opportunity anymore. On top of all that 3commas offers back testing, dollar cost averaging BOTS, a ton of different trading tools, a traders diary to keep all your trades in one place and a highly developed signals marketplace which allows you to mimic and automate the trades given by the top signals providers. That means you can follow them signals and let the bot do the hard work. 3commas has not forgotten about mobile users too. Just hit that App Store and you will see that the bot supports all sorts of major exchanges such as KuCoin, Binance, Binance DEX, Binance Futures, BitStamp,EXMO, YoBit, GateIO, CEX.io Coinbase Pro, OKEX, Bitfinex, Poloniex, BITtrex, HitBTC Kraken and Huobi Global. Cost wise, 3commas offers a free three day trial and prices range from anywhere between $14,50 per month and $49 50. If you are not into futures trading then the plan for $25 is what you want. Onto the pros and cons, in my opinion 3commas has one of the best interfaces out there. It's got copy trading supports a ton of exchanges and offers that sweet signals marketplace. On top of all that I cannot stress how useful that smart trading feature is. 3commas is probably not the best pick for inexperienced traders. So if you're an experienced trader looking for all the bells and whistles, you need look no further than 3commas. As mentioned before one drawback of using these bots is having to keep your funds on an exchange. Which of course does have its risks but there is no getting away

from that if you want to use them. So if you're going to be running trading bots then I do recommend that you split your funds across more than one exchange. These bots support multiple exchanges which makes it easier to spread that risk. Also if you're going to be using a bot that I haven’t mentioned before, make sure that you do your research and extra suspicious of any bots that promise returns. There have been a number of instances in the past where API Keys have been phished in order to conduct malicious trades so be aware of that. In the end crypto trading BOTS definitely won't make you a millionaire, but if used correctly they can equip you with the tools to improve your trading game. To learn more about 3commas, please visit their website at https://3commas.io/

Chapter 12 Key metrics signals & Red flags

Imagine that your mate just told you about this super-hot hidden gem of a crypto that's about to 1,000 times and take you to the moon. He seems convinced and has you on the edge. You're training accounts is open and ready to buy some. But how do you know that you're not about to buy a sh*tcoin? Indeed, how do you even know what a sh*tcoin looks like? In the following chapters I'm going to tell you exactly what to look for, some key metrics signals and red flags that should have you running for the hills. I'll also be letting you know about some top tools that I use to screen out these bad apples while doing my due diligence. Before I dive in I want to lay some groundwork before we start this analysis. I know some people can get testy when you claim that their moon sh*tcoin is a junk and some of these bag holders can be pretty emotional. So I need to point out that if a coin or token meets one of my sh*tcoin criteria, this does not mean that they should be immediately dismissed. Those coins that should be viewed with suspicion are those that meet many of these criteria. Indeed there are many projects that may take one or two boxes but could still be pretty good for the long term model. So at the end of the day you have to decide on where you sh*tcoin alert will be triggered. With that out of the way, let's start with the sh*tcoin sitting. I'm going to start with a top-down approach. This saves you time before you start digging into the weeds of the project itself. The first thing I tend to look at is also one of the most obvious and that is exchange listings. Simply you can tell a lot about a project by which exchanges their token trades, or if it has much exchange support at all. Why is this? Well quite simply most reputable exchanges don't want to be associated with coins that they deem to be useless. By that I mean they don't want to have a lot of angry traders coming to them because they lost nearly all their money on some vapourware project. Moreover it also creates certain problems for you buying the cryptocurrency. How can you feel really comfortable using some exchange that you've never really heard of just to buy that rare altcoin someone flagged? So if you're analyzing some low market cap old coin and you see that there is very little exchange support that should be a concern. It should also be a real concern if it's listed on some exchanges that are known to be on the dodgy end of the spectrum. I can't go over all of the shady exchanges but there are a number of sites that can conglomerate this data.

You can use Coinmarketcap but you should be still skeptical of trusting their exchange rankings. Still, there are some decent alternatives. One of those go-to sites for me is called CoinGecko. Much like CMC, this is a another market cap aggregation tool. But what I'm really interested in is their exchange rating tools. Here you can see a list of the top exchanges and their trust score. If you're looking into an exchange that lists a coin you're considering, then you can just search for it here. Then you'll be given the trust score and you can make a judgement on that. Of course you should not take the CoinGecko trust ranking as some Bible. You could also just take a look at what other users have said about the exchange online. Dodgy exchanges do eventually get called out. To check out CoinGecko, please visit the site at https://www.coingecko.com/en Or, if you want to take a look at Coinmarketcap, please visit https://coinmarketcap.com/

Chapter 13 Volume & Liquidity

Moving on, assuming that the coin is listed on an exchange that is relatively reputable, you need to make sure that it is actually being traded. The volume and liquidity of a token is important to study. Not only can it give you a broader indication of interest, but it will also help you determine whether you will be able to easily buy or sell the cryptocurrency yourself. Let's start off with the volume. You can easily see this data on sites like Coinmarketcap or CoinGecko now the trading volume of a cryptocurrency should not be viewed as an absolute number but rather as a proportion of the market cap of the coin itself. Any coin that has a 24-hour trading volume that is less than 5% is considered quite low. But even if the volume tends to be healthy for 24-hour period, this could be a trick. That's because volume can easily be artificially manipulated this is especially the case for those dodgy projects that want to make their trading appear active. The term is wash trading and it’s dodgy. Trying to spot wash trading can be quite difficult. There are a number of order book red flags that you should be looking out for. I have explained washtrading in detail in my other book called Bitcoin and Cryptocurrency Trading:Must have tools, Best Exchanges and Trading Strategies. You can also use another quick tool over at CoinGecko. You can click on the coin in question and you can select the market section. This gives you an overview of the liquidity, across all the exchanges where it's listed. You can just take a look at that trust score column to get an idea of whether the trading pair has decent enough liquidity. If most of the pairs of the coin on CoinGecko appear to have low liquidity, then it could be a sign of a low interest aldcoin, not something you want to buy. That does it for some of the coin market metrics, so now let’s take a look at the development activity.

Chapter 14 Project & Dev Activity

If the project appears to be relatively well supported with decent liquidity, then you're going to want to take a closer look at its development. Something that I always do when analyzing a project is to take a look at their public code repositories; their github or get labs. If their code is not public, that could be a red flag. Some projects developing private repositories before pushing live, but you cannot verify this. Moreover, cryptocurrency and blockchain technology is about transparency. All of the most successful crypto projects have open source code. If they do make their code public in their reps, then you'll want to observe how much has been done over the past few months. You don't have to be a developer to do this. You just want to see that there has been a regular stream of commits and discussions. If it's unproductive and thin with virtually no activity, then that should set some alarm bells ringing. What are the developers been doing in the past few months? While we're on the notion of activity you'll also want to take a look at whether the project has been active in other spheres. Do they have a blog and is the team keeping the community updated? What about some of their social channels? Do they update their Twitter regularly and can you see life over there? There needs to be a balance. No one wants to see a meaningless tweets for the sake of tweeting. An announcement of an upcoming announcement, but if the team has not found anything useful to mention in the past few weeks maybe they're not doing anything useful. Speaking of the team, here's a great segue into my next subject to explore. A project can have all the right ideas an amazing use case and great community support, but if the team is sketchy you can be pretty sure that that will feed into the project. Sketchy is a pretty broad term that encompasses a number of different factors. Firstly, are the team who they claim to be? Can you confirm their credentials on their social platforms like LinkedIn? Have they been involved in any questionable projects in the past? How long have they been involved in the blockchain space and is their background relevant for the project? Relevance is also a bit more nuanced but you can be a fair judge of this. If the whole team is made up of X marketing folk who know how to type, then I'm a bit less inclined to support it. In the world of crypto projects cutting-edge tech is what gets you above the crown. If most of the team members are not technical then how can we be sure they know what to develop. Also if there's one thing that we've seen in the crypto

space so far, a good marketing strategy can push vaporware projects to astronomical highs. The simple rule of thumb is this. If these guys were pitching for an investment in their seed ground startup, would you feel comfortable investing in it?

Chapter 15 Comprehending the Project

Let's assume that the crypto has managed to pass most of your high-level criteria it's time to dig a little deeper into the project itself. The first thing that you need to ask yourself when looking at the project value proposal is; does this actually need a token or cryptocurrency? There are numerous examples of projects that have developed a cryptocurrency for something that really did not need one at all. Let's not forget that the future value of a utility token will come from its actual use. There are projects that I've seen that have developed a cryptocurrency for dentists, farmers or sports stars. This question of token utility becomes even more relevant for those projects that have completed ICOs or built on EtherEum. If you really need people to transact in your network why can't they just use ETH? Why do they need to use your token? Being able to stake on the network is not a legitimate use case. Why should I expect any sort of price appreciation and value from your token when I can just buy a Ethereum and capture all the additional value generated from network use. So if a project has a token or coin just for the sake of it, you have to wonder whether it could ever face mass adoption and be worth a lot more in the future. Speaking of use cases, this then brings us onto the topic of business development. At the end of the day a theoretical use case is nothing unless it's been put into practice. You need to take a look into the integrations and partnerships that the project is either engaged with, or working on. This could give you a sense of how they envision the token so eventually being used or mass adopted. Are these partnerships meaningful or are they merely a partnership for partnerships sake? A simple collaboration, or memorandum of understanding? Something that's concrete, or nothing more than a simple meeting. I have seen far too many projects that overhype a partnership that is either completely false or extremely misleading. There have been examples of cases where the other side of the arrangement needed to come out and further clarify the exact nature of the partnership. Of course a project and cryptocurrency may still be in it's relatively early stages and businesses or developers may not have started integrating yet. That's totally understandable. But do they have a strategy to increase adoption? Have they outlined a broader commercialization strategy? Far too often teams will claim that their blockchain project and cryptocurrency could disrupt an industry, but they don't have the first clue about how they're going to do it. This just

shows that they were never really all too serious about the adoption and the more driven by hope. So make sure that they have some plan on this front. Assuming that the project has been around for some time then you have a lot more information to go with to help inform your opinion. This is where track records speak volumes. So you need to ask yourself if the project has some consistency in its vision. Those projects often change their focus and reinvent themselves every single year, almost definitely wants to watch out for. If their previous core use case is no longer a strong one what is to say their new one is any better? Moreover if they could not execute on their previous strategy why should you have any confidence that they're able to do it with the new vision. I have seen it all. Projects that started out as a development blockchain that would be an Ethereum killer then switching their focus to blockchain storage or supply chain tracking. Completely flipping the script as if that is supposed to inspire any confidence. Projects like V-chain or Chain-link had one vision strategy and focus that has defined them from the beginning; consistency. The same can't be said about projects like Factom for instance who constantly shifted the goalposts and eventually ran out of funds. They recently filed for chapter 11 bankruptcy protection. Also while we're on the subject of consistency, this is not just about the broader vision and use cases. It's also around its development goals and roadmap. Do they often missed milestones and have some of these proposed milestones just vanish from the ether? Sometimes I wonder if some development teams even know that an old roadmap can easily be pulled up and analyzed for progress. Reading over their old road maps and white paper is an important point of the analysis, at least at a glance. These initial documents can help me to determine how things have changed. If you read their latest roadmap and they have really grand visions, you can place that in the right context when viewing their old ones. While we're on track record, there is something else that you can observe for all those projects that raised an ICO and that is how that money is being spent. Of course, you might find that the team isn’t tell you what they're spending their money on. Well, that should kind of answer the question. Most legitimate projects with a foundation will have detailed reports as to where the funds are being allocated and what they're being spent on. If no such disclosures exists then it's an immediate red flag. If they don't want you to know what the funds are being spent on. well there must be a reason. Then for those projects that do disclose this, you need to ask yourself whether it falls in line with their white paper budget allocation or whether it

is at all justified. Let me give you a few examples to illustrate this. For example a project called Sirin labs raised a total of 157 million dollars in an ICO back in 2017. The goal was to develop a blockchain phone. They issued their own token in the ICO which of course asks the question; was a token even needed? The CEO have spent a fortune to get a Messy sponsorship of their phone. It seemed to be all good until you realized that the phone itself, well, no one really wanted to buy it. Sirin labs burned through all of those ICO funds pretty quickly to the extent that they had to lay off half of some of their workforce. A 157 million dollars gone. What did they spend those funds on? Well, no one really knows. I don't mean to take stabs at these projects. Just wanted to give you guys some concrete example of irresponsible spending of project funds.

Chapter 16 Artificial Perception of Demand

Speaking of irresponsible allocation of funds to more metrics that I want to mention are the page shell factor and sock puppet index. Those crypto projects that have to rely on page shells to pump their coin or token should be view with immense suspicion. Why should they feel the need to create an artificial perception of demand? Does that mean that there is no real organic interest in the project? So what do these shells and sock puppets look like? Well they could range from a very well-known influencer all the way down to those individuals who always spam and comments on forums and other platforms with shameless project plugs. When it comes to the latter, these are either basic user accounts or merely bot farms that spread the project around. It just screams of desperation and it is a major turnoff. Don't get me wrong, projects are perfectly entitled to pay for coverage from influencers and other alternative media channels. However these should be fully disclosed and transparent. Honesty is the best policy. And those projects that try to manipulate the narrative, should be on your sh*tcoin shortlist. As mentioned just because a crypto meets one or even two of these criteria does not necessarily imply that it should be avoided. There could realistically be a situation with a coin that's just new to the market and with very limited exchange support and volume, but is singing all the right tunes when it comes to the other criteria. Indeed newer and relatively less hyped projects may not have the coverage of established altcoins, but they could still be hidden gems. So when using these criteria, it's important to view it holistically. I also encourage you not to use the term “scam” too liberally. Just because a coin is junk, does not mean that it's a scam. It does not mean that the developers or creators have any malicious intent. It just means that they've developed a cryptocurrency that is not valuable, unique or in demand for anyone else. And that is not a crypto you want to hold.

Chapter 17 Crypto.com: Interest earning tool

With over a million downloads, it's safe to say that the crypto.com app has been taking the world by storm. What's all the fuss about and should you bother giving it a try? Well, in the following chapters I'm going to go over everything that the crypto.com app has to offer. All that is to help you decide if it's the right choice for you. The first thing I want to talk about is the apps integrated multi crypto and Fiat wallets. You can find this crypto wallet in the app by opening up the home screen and clicking the little lion at the bottom of the screen. Then just tap the wallet tile and you'll be in the crypto wallet section of the app. Here you can store over 80 different cryptos. That's a lot of coins and chances are that the cryptos you want to store will be supported here. Like any other crypto wallet, you can send or receive crypto. You can do that by clicking on the transfer button. Click deposit, if you want to send crypto to your crypto.com wallet. Then choose the crypto currency you want to deposit. Then you'll see your crypto wallet address to send to. When it comes to withdrawals, there are two major things I need to be upfront about. The first is that there is a fee to withdraw to non crypto.com wallets. The problem is that there is no functionality to adjust the transaction speed and fee. Instead it's set at a flat rate and there is nothing you can do about it. For Bitcoin this is set at 0.0003 Bitcoin which is just under 5 dollars. That’s not really good. How to actually withdraw from the crypto.com app? Well, in that crypto wallet section you'll need to hit that transfer button and click that withdraw button. Then select the type of wallet do you want to withdraw to. You'll then be asked to whitelist the wallet address you want to withdraw to. Click the little plus sign in the top right corner then just select the crypto you want to withdraw and input that address. Once done you'll get an email from crypto.com asking you to confirm and authorize that wallet address. You'll then be able to withdraw to that whitelist as well as address and all you need do is key in the withdrawal amount and click on withdraw. Moving on, the crypto.com also has a Fiat wallet too. This allows you to buy crypto with a bank account. Up to 21 different fiat currencies are supported but some of those might be restricted depending on what country you're based in. So if you're searching for an alternative way to get into crypto currency, then you can do that with the crypto.com app. But what about the fees? Well, the good news is that crypto.com doesn't charge you a fee for deposits all withdrawals

using Swift bank transfers to and from the app. The bad news is that your bank may charge you between 6 to 40 dollars for a transaction. But what other features does this app have? “Crypto earn” essentially allows you to lend out your crypto on the app and earn interest. Bear in mind that your typical bank account pays out less than 1% interest per year. It's pretty easy to see why so many people are flocking to crypto earn, when you can get an annual interest rate as high as 18%. What's important to note is that the interest rate for supplying crypto on the app varies according to the crypto currency you supply, the lending term and if you have 500 MCO state or not. 500 MCO is not cheap and will set you back over 2500 dollars. However if you have that stake within the app you'll get an additional interest bonus of 2% on fixed term deposits. So to get that 18 interests you'll need to have those MCO tokens state within the app. The other thing to be aware of is that interest rates vary according to the crypto asset you're supplying. With stable coins you can get up to 12% interest. 18% if you supply CRO and you can get up to 8% with other assets. So if you're interested in getting the highest interest possible then you better go with CRO. the final variable is the length of the staking term. the crypto.com app gives you three different options. tlexible staking is naturally the most flexible plan. it provides a low risk saving solution that allows you to test out the waters and withdraw your coins at any point with no penalty fees. lock your coins up for one month and you'll be rewarded with more interest and you'll get the maximum interest rate if you commit that crypto to be locked up for three months. On top of all that you'll get an additional 2% bolted on if you have 500 MCO state. So that's how you get up to 18% max interest here and one of the reasons why you might want to stock up on some CRO. All this sounds amazing however you should know that MCO and CRO are both crypto currencies issued by crypto.com. Another cool feature of this app is the ability to get an instant crypto loan, using the crypto credit service. Applying for a conventional loan you'll know that it requires a ton of paperwork and that it's extremely slow. With crypto credit, there are no annoying credit checks at all, no boring forms to fill in, and it's instant. So what wizardry is this? Well these loans are over collateralized loans where you can supply Bitcoin, Ethereum XRP or Litecoin as collateral and get 50% of its US dollar value in stable coins like Paxos, Tether USD coin and Tru USD in return. Interest rates start at 12% per year. But you can drop that down to 8% if you're staking 500 MCO coins. Another thing you need to know is that the credit duration is 12 months. Before you

jump right into that crypto lending it's important to understand how over collateralized loans work before you consider using them. These types of loans are similar to getting a loan from your local pawnbroker. That's where you take an item like a car, jewellery or pretty much anything of value to the pawnbrokers and receive a loan based on the value of the item. The pawnbroker might lend you 50% of the value of the item, charge you interest and if you miss your repayments, they might sell your item to recoup the value of the loan. As pawn brokers always lend you less than the value you're putting up for collateral, the loans they provide are always over collateralized. Crypto credit in the crypto.com app works in a pretty similar way. You bring that crypto collateral which is then locked up and you receive 50% of that collateral value in stable coins. We all know that crypto markets can be volatile so it's important to be aware that if the market price of your collateral falls too much, then you'll have your crypto liquidated by crypto.com to cover the value of the loan. It's very much like a pawnbroker selling an item to cover the cost of the loan that's gone south. In other words if the crypto price moves against you by 50%, then you could lose the rights to that crypto you've supply and be left hodling stable coins. The next app feature I want to talk about is called “crypto pay” and that's all about buying stuff with crypto. One cool thing you can do here is buy gift cards for over three hundred bands with Bitcoin, Ethereum CRO, XRP and Litecoin. If that wasn't good enough, you can also get up to 10% cashback if you use CRO to buy them. The exact level of cashback depends on a few factors including what type of gift card you buy, if you have an active fixed deposit term of greater than 10000 CRO or if you've staked more than 10000 CRO in the crypto.com exchange. So if most of your money in crypto, you might find things like supermarket gift cards particularly useful. That's all the more sweet up when you're getting 5% cash back rewards too. Crypto pay also includes something called airtime, which allows you to top-up your mobile phone, using crypto or if you're feeling generous your friends. The final thing that crypto pay has to offer is a scanner to allow you to spend your crypto at any supported store. Just scan that QR code and you'll be making that crypto payment in no time. Another neat feature of the app is its crypto tracking function. Most people do not know this but if you click the account button and hit “pie chart” in the top left-hand corner, then you'll get a nice visual breakdown of all the coins you hold on the app. A pretty cool way to track your portfolio. If you want to make sure you keep your finger on the pulse of

the crypto markets then this app also offers a handy alternative to Coinmarketcap and gives you all that price data for the top crypto currencies. You can also click into different coins to see price graphs and more detailed stats. Pretty useful. Another great feature here is the price alert function. Hit that Bell for any cryptocurrency and you'll get push notifications if there are any major price movements. That means you'll be the first to know if there is a price break out that you want to trade. To learn more about the app, please visit their website at https://crypto.com/en/index.html

Chapter 18 Crypto.com: VISA Card with Cash back

Now it's time to talk about the main reason why most people use the crypto.com app. That would be getting a crypto.com card. The first thing to know here is that you can only get your hands on one of these crypto cards if you're based in the US, UK, Europe, Canada or Singapore. The second is that they support Bitcoin, Ethereum, Litecoin, XRP and MCO. So if you like the idea of being able to spend any of those cryptos using a Visa card, then this is going to be for you. The key question is which one should you choose? There are five different card tiers and if you're interested in knowing all the details about every card then check out their site within the card Compare tier list here: https://crypto.com/en/cards.html

However I'm going to go over my top two card picks. After all I don't think many people would be that interested in learning about the black obsidian card which will set you back over a quarter of a million dollars to get. Honestly I think the crypto.com blue card is a no-brainer for anyone in crypto. It's completely free and I cannot see what anyone has to lose by ordering one. In terms of perks, you're looking at 1% in crypto cash back on all purchases. One thing to note here is that all cash back is paid in MCO coin. Not that big a deal seems it's the top 100 cryptocurrency with a ton of trade volume and supported by numerous exchanges. So what else can you get with this card? Well, you can withdraw up to $200 per month from an ATM for free. However be aware that you'll be charged 2% for cash withdrawals over that amount. Pretty ideal for a casual crypto card user. Another thing that's great is that if you manage to go abroad you can access interbank exchange rates with a monthly exchange limit of $2000. I don't know about you but whenever I go on vacation I shop around for ages trying desperately to get the best exchange rate. That's a thing of the past with this card is that interbank rate is pretty much going to be the best rate you'll ever get. Here is my favorite crypto card called the crypto.com Ruby card. To get it, you'll have to stake 50 MCO tokens in the crypto.com app. This is just over $250. The important thing to know is that these tokens are only staked and you can get them back later. So it's a very different situation to annual card fees. With that barrier to entry what do you get? Well, right off the bat your crypto cash back is doubled to 2%. That's honestly more than what Amex used to give back in the day for a ludicrously expensive credit card.

You'll also get a free Spotify subscription too. That rebate is paid into your crypto.com wallet in MCO. What Spotify worth? Well in the US this will set your rack around $9.99 a month. So in a year you can expect around 120 dollars' worth of value from that free Spotify subscription alone. When it comes to maximizing those cash back rewards, here's my little secret. I personally try and run every possible transaction through this card to really take full advantage of those rewards. So if you easily spend $1,000 a month on just surviving, then you could have 12,000 dollars in transactions running through the card a year, which equates to about two hundred and forty dollars in crypto cash back. All that for simply choosing to leave that fiat card at home. Another thing I really like about this card is that it's made out of metal. There seems to be something super alluring when you slap down a metal credit card to pay that bill. What I can almost guarantee is that heads will turn if you flex that metal card. Free ATM withdrawal limits on this card are raised to $400 month and you also get access to 4000 dollars' worth of interbank exchange rates per month. So what's the value summary for the Ruby card? In the year you'll get 120 dollars in value from that for Spotify subscription, 2% in crypto cash back and that metal Visa Card. After running that through the value calculator I come to the sum of 360 dollars in value. Not too bad if you ask me.

Chapter 19 Crypto.com: Trading tool

The last app feature is the trading function. You can access that on the home screen by clicking the trade button. Selecting buy or sell, choosing the crypto you want to trade and execute in that order. It's honestly, that simple. However I do want to share a few closing thoughts. The first thing I want to address is whether crypto.com is legit. I'll be honest with you. There are some out there that believe that crypto.com could be a giant Ponzi scheme. After all their crypto credit service offers some of the highest interest rates in crypto. Well what I will say is this crypto.com have been working on building their ecosystem for years. They acquired the crypto.com domain for over ten million dollars and have partnerships with the likes of Visa and Ledger. Let's also not forget that your fiat bounces are covered by FDIC insurance. So I think it's highly unlikely that crypto.com is some form of ponzi scheme. All that being said there are a few things I don't like about the app. The major one is that the crypto.com wallet is completely centralized. That means you do not hold your private keys and you're trusting crypto.com with your funds. There are rumblings that the team are trying to decentralize all that, but as things stand it's a centralized wallet so just be aware of that. I also really dislike the Fiat withdrawal fee to withdraw to an external wallet. Crypto.com is upfront about that but I don't like that one bit. When it comes to crypto tracking I need to level with you; there are far better options out there like Delta or Blockfolio which I have discussed in my other book called Bitcoin and Cryptocurrency Trading for Beginners with the subtitle of must have tools, Best Exchanges and Trading Strategies. Another thing that is deliberately obvious is that crypto.com is using this app to drive the demand of their MCO and CRO tokens. Basically to unlock any worthwhile features you'll need to get your hands on some. I understand that token utility is super important however it would be nice to be able to get a crypto.com card using Bitcoin or some other crypto. All things being said, there are a host of features and top-notch functionality in this app and I'm sure many of you will absolutely love it. I have to hand it to the Devs at crypto.com the interfaces are super slick and straightforward to use.

Chapter 20 100x Altcoin Research: Screening Process

Assume you want to pick an altcoin gem. That next low-cap cryptocurrency they've got 10, 20 or even a hundred times and take your crypto portfolio to the moon. I know many people who banked a stack full of cash from investing in undervalued and hidden altcoins. However in today's idiosyncratic markets that has become a lot easier said, than done. So then how do you find those hidden diamonds in the crypto market? Well, in the following chapters I will explain exactly what you need to know to do that. I'll take you through some methods that have been used by various people and made them rich. There are a lot of altcoins out there. Too many to count. Most of them are sh*tcoins But those golden nuggets do exist. You need to start the process of finding those golden nuggets with a top-down approach. An extremely simple initial screening mechanism to get a shortlist of coins that you want to drill deeper into. Perhaps the simplest of all these is market cap. This is because it's easily available for all kinds and there are a number of tools that track this info quite effectively. It's also essential for your selection of the coins you want to target as you can immediately eliminate those that you know not likely to really ten times or so in the near future. You need to find those coins that have really small market caps and hence have the most opportunity to really grow like that. For example if you take a look at all those coins in the top 100 of market cap over at CMC, it's pretty unlikely that these will increase as much as a coin that is sitting at around 300 in market cap. Why is this? Well it's just simple maths. You're already starting at such a high base. It's a lot harder to take a project with a market cap of 50 million to 500 million, than it is to take another coin with a market cap of 2 million to 20 million. So will then have to set out an acceptable range that we think our altcoin gem could be in, and then eliminate all those that are not candidates. There are a number of market cap tracking tools out there including Coinmarketcap, CoinGecko or CoinCodex. For this screening process I usually use Coinmarketcap. This is just because they have a pretty neat filter where you can select the market cap range. You can also drill down further with other metrics something which I will explain in a bit. Generally I like to look at those that are below 10 million dollars in market cap. This should give the coin enough Headroom to really multiply in price should its real value be realized in the market. I usually have a lower bound of about 5

million dollar market cap as well. It's not a hard stop, as there may be a few interesting projects below this cutoff. However the bulk of coins below this market cap are sh*tcoins. They have very little adoption and awareness and even if they have great tech, they're being crowded out.

Chapter 21 100x Altcoin Research: Trading Volume & Exchange activity

So now I have my list of coins that I can start focusing in on. This then calls for another filter to further clear the field. The next metric that I'll look at is the volume. This is an important metric as it shows just how active the trading of the coin is. It can also be a great way if you to spot coins that have artificial or abnormal value. Those that may have some wash trading going on. So I like to look at those coins that take about two to six days to turn over their market cap. Put another way, the 24-hour volume should be between 10 to 50% of the market cap. You can't filter a ratio of two metrics on CMC, but you can easily just copy the data over to a spreadsheet and run your own custom filter over it. You can develop a simple Google sheet where you can manually copy the data into. There are ways to develop dynamic screening tools on CMC that use the API but these don't work too well for the lower market cap altcoins. Once you have the ratio of the coins volume to its market cap, you can also run an Excel filter over this so that you are only looking at those coins that you want. Those with a ratio of between 10 to 50%. After applying this filter I have the about 50 altcoins which I will further have to investigate. I need to make absolutely sure that the volume is completely legitimate and not compromised of any wash trading. We've already screened out the most of the coins at wash trading by zoning in on the volume. However to make doubly sure we also have to look at their exchange listings. Indeed seeing where a coin is listed is another important metric as you are after all going to be buying it there. You want to know that you can easily get your hands on and liquidate when you see fit. Here, if a coin only trades on one exchange with a dodgy track record then you should avoid it. Moreover if a coin is to really rally in price, it has to be on an exchange that has a large user base. An exchange where more people get exposed to it are aware of it and can consequently buy it. For browsing through the best exchanges I prefer to use CoinGecko as I find their rankings to be a bit more independent. So now you should take one of the coins you currently have in your refined list and take a look at the exchanges where it's listed. Next, hop on over to CoinGecko and search for the coin. You can select markets and this will show you a list of all the exchanges where the coin is trading. You can see that CoinGecko assigns a trust score to these exchanges. If you see that the coin you picked volume is currently taking place on an exchange you

might have never heard of and they are not your top pick that might be already a red flag. However you can also just take a look at that market depth. Market depth is another way to think about liquidity. Those coins that have deeper order books have more liquidity and hence are easier to trade with larger block orders. However if you see that it is listed on Binance that could be potentially good. Most can agree that Binance is a pretty reputable exchange with deep liquidity and reasonable volume. It also has the highest web traffic among the exchanges and the most users. So this is a great sign for the future potential trading of the token. Those are most of the market metrics that I use to zoom in on the coins that are worth doing a bit of deeper digging.

Chapter 22 100x Altcoin Research: Onchain Metrics

Once you have this list, you can take a look at some important network metrics. Onchain metrics are important. They show whether a cryptocurrency is being used. Whether it's active and not just a nice concept. There are a number of metrics that you can look at here from address activity to network participation on staking coins to total transactions. In fact there are so many metrics to look at that it could be hard to have positive signs from all of them. One cannot really use the same network valuation metrics for all coins like this than they do for large cap old coins. There are a number of tools that you can use to see these stats but one of the best out there has to be IntoTheBlock. Their website is at https://www.intotheblock.com/

They have a overabundance of data and it's not just resigned to network metrics. They offer a 7-day free demo but the paid packages are not that bad at all for what you get. The first metric you should be looking at is the percentage of active addresses compared to total addresses. This can give you an idea of how many people are really using the network compared to how many are just sitting with their tokens in the wallets. Activity in this case is of course transactions to and from said address. As you can know that tell those are the very low ratio are less desirable. Of course you could have a situation where both addresses and transactions are increasing at the same rate in which case the ratio will be constant. So you can also take a look at both of these ratios independently. If both are growing, that is a good sign. Another neat stat that IntoTheBlock has is the time between transactions. This is another stat that you can use to give you an idea of just how active this blockchain is. Moving away from unchanged stats you will also want to possibly examine the distribution of tokens on the network. Centralization is generally not something that you want in a project as it means that Wales can control the market.

Chapter 23 100x Altcoin Research: Development Activity

Now that we have been through some of the most important on chain metrics that help you determine how active the network is but what about a development activity. This is why I like to dive into the github repos of a project. It's perhaps one of the most transparent ways for me to ascertain development activity. One of the only ways that an altcoin can separate itself from the crowd is with impressive tech and this needs to be worked on constantly. It's not really about being able to read the code that underpins the protocol. You just want to see a regular stream of commits in the core repositories. You want to make sure that there is active discussion in these repositories. If they link to their github then you can go over to the insights section and you'll see the commits, code frequency and contributors. If your token is active with a regular stream of commits and additions or deletions that’s great. You can then head on over to the issues tab and see the discussion around the code additions. I should caution you that sometimes you don't get the full picture of development on the public code repositories. Not all commits are created equal and often developers or code in private repositories before they push it live. If you think this could be the case then you could head on over to their development Docs or blog to see what they say about it. Now we've been through the screening process without even looking at any of the projects. This is why important to have a top-down screening process in order to zoom in on those projects that could be interesting. The next stages of the analysis actually involve doing due diligence on the projects themselves and that takes a lot more time. Now that we have our list of projects that we want to research we can finally look into some other specific information. If you know many investors in the venture capital realm, you'll hear that on many occasions they mostly back the team. If the startup has a great team then that's already a major hurdle cleared for the startup business plan itself. As such, you should also place a large emphasis on this when initially doing your research. A team comprised of individuals who have a background in the space is really important. You should also make 100% certain that all of their information is publicly available and verifiable. I remember back in the 2017 ICO craze when fake team credentials were used to promote a project. It‘s important to verify credentials. Check out their LinkedIn, github, Twitter and other social 's.

When doing so it's also important to make sure that their skills and background are aligned. I generally prefer it when a project has a developer heavy team. This is after all is all about cutting edge technology so this should be a preference. It does also help to have people on board who have a business or marketing background as they can help forge partnerships, which could increase adoption and awareness. However unusually a bit turned off when most of the team members are marketers and self-aggrandizing shills. We have enough of that in crypto. There are still a few projects including a pretty well-known one that have pseudonymous developers. Satoshi did create the most valuable blockchain in the world but in today's day and age it helps to know who is behind a project. There is a sea of ICOs that manage to exit scam because no one knew who they were.

Chapter 24 100x Altcoin Research: Project Uniqueness

Once you've done your research and are pretty happy with the team behind the project, it's time to look at the white paper. I know that many people try to avoid reading over the white paper but this is a shame. There is so much important information that you can glean from doing so. Moreover, a really fluffy white paper could be another sign that you should avoid it. You should also read it with a pinch of salt as it may not be fully updated. However it's an important first step in order to get a vague understanding of what the project is about. You don't have to study it inside and out, just have to focus on some of the most important points and whether they make sense. Some of these include; consensus method, technology stack, interoperability, scalability, use cases and roadmap. Let's take a look at each of those individually. The consensus method is important as this helps us determine not only how secure the blockchain is but also whether it's scalable. There are a plethora of consensus protocols out there with our own pros and cons. Some are pretty unique and ingenious. Others are more plain vanilla. It's an important factor you should consider. The technology stack is a pretty broad term but it means the general structure of the network. How broad is it? Are there numerous different layers where additional technology and functionality can be built? How does this technology stack make the project unique amongst all of its peers? Interoperability means a protocol can interact with other block chains and networks. This could help the network access liquidity and applications from other ecosystems. While the project may not be completely interoperable to start, it's great to see a plan to reach that holy grail of connectedness. Scalability is mentioned quite frequently, but simply if a network cannot scale then it will eventually suffer bottlenecks. This is something that we see with some of the most popular blockchains today. If a project has a consensus method that is scalable, then that is a plus. But will they also develop other scaling solutions? Perhaps off chain etc. Use-cases is pretty self-explanatory. The only way that you're really going to get adoption for a network and the currency is whether there are defined and reasonable use cases. You also have to ask yourself whether these use cases make sense or are just a bunch of gibberish. For example who needs a cryptocurrency for dentists? Well, there is a coin that exists for dentist, yet no dentist using it. Finally, we have that roadmap. This may not always be up-to-date in the

white paper so I do encourage you to take look on their website if they have it. But basically a road map is an essential part of a growing project. It's one thing to have a theoretical construct of what you want your network to look like, but it's another thing entirely to execute on it. Are there defined goals and timelines in the road map? Is it detailed enough to be able to measure their performance in meeting these goals and timelines? Based on previous milestones, have they met them or constantly pushed it back with delay after delay? While we're on the point of delays I understand that it's sometimes hard to keep to a defined timeline when developing such a promising tech. But there has to come a point where a project has to be adequately penalized for missing these guidelines. There are some projects today that despite having completed ICOs back in 2017 have still not released a main net. As mentioned a lot of this stuff may not be available in the white paper and it may be dated. That is why you should then take a look at what has been going on with the project since it's been released. Apart from the activity in the github, you can also take a look at their blogs, social media and other communication channels to see where the project is going.

Chapter 25 100x Altcoin Research: Adoption & Community Support

Something else that can really help increase the awareness and adoption of a cryptocurrency is of course the community. How big is it and how active are the members. There are a number of simple tools that you can use to ascertain the size of the following. If you head on over to CoinGecko you can get a sense of just how many followers there are and how active these users are. You can also head on over back to Chainlink's website and dive deeper into their social stats. There is an entire section for that there. Of course for smaller communities and projects the data can be thin. That's why I like to dive a little deeper in order to determine exactly what type of community this is. The dedication of a project community speaks volumes about the broader potential. When you jump into the telegram groups or read through the forums you can easily get a sense of what type of community you are dealing with. Is there a lot of thoughtful discussion going on? Are the users genuinely interested in the technology and adoption of the network? Are they helpful and welcoming to new members? Do they help answer some of their questions? These are all strong community signals. If however you see a flood of memes and personal attacks, it raises a few red flags. People who throw around the word FUD for a lack of a solid argument, just turn me off of a project. Why is this important? Well a community that is passionate about the project has staying power. They're interested in seeing the cryptocurrency adopted and know the exact reasons as to why it will be. They're also willing to spend the time to make sure that others are aware of the project. It's also known as free marketing. In summary, there are my main criteria that I use when screening for altcoins. There are other factors that I take into account too but I do hope that you are able to use some of these methods to screen for your altcoins. Remember, time is money and if you're able to zoom in on those projects with the most promise really quickly you're already on the right track.

Chapter 26 Trading Tips: Option Moneyness

We are all in search of that hidden edge on the markets. That slice of information that when used appropriately can give us outsized gains over the rest of the crowd. The only problem is that most of this information is reserved for a chosen few. Either that or it's ridiculously expensive to attain. But what if I told you there was a cheap and effective way to get hold of this. A free resource to better read the Bitcoin markets and be two steps ahead. Well, in the following chapters I'm going to explain how you can use the Bitcoin options market to your advantage. Not only when it comes to option analysis but also when trying to determine Bitcoin's price direction. All that is to help equip you with the tools you need to get the market edge. I want to start with a quick beginner's overview of options. An option is a financial instrument that gives the holder the right to buy or sell an asset at a pre-specified time and at a pre-specified price. A call option gives you the right to buy the asset, whereas a put option gives you the right to sell the asset. Because these options are instruments that give you optionality there is a cost that comes with them. This is the option premium and it is the price of the option. Options are themselves derivative instruments that are traded on their own market which is separate from the spot market. You can think of it as analogous to the futures and spot markets. There are a lot of variables that will impact on the premium of an option. These are collectively called the “Greeks” and they are inputs into the legendary black skulls pricing equation. If this appears daunting to you don't worry. All you need to understand are the main drivers of an options price. The first thing that i want to introduce you to is the moneyness of the option. This refers to whether an option is in the money or out of the money. Basically, if you're looking at a call option if the spot price “S” is above the strike price “K”, then the option is in the money.

Example: S > K options is in the money or ITM.

Conversely, if the spot is below the strike it is out of the money. Example of that is: S < K Options is out of the money or OTM.

When you have the strike equal to the spot then it is at the money. An example of that is: S = K options is at the money or ATM.

For a put option you just flip the arguments for the in or out of the money

levels. The moneyness of an option is important as it impacts on the delta variable in the black skulls. Delta is a measure of how sensitive the price of the option is to a change in the price of the underlying asset. Then you have other factors such as the implied volatility. This is also a very important input in an option price and generally the higher the implied volatility, the higher the price of the option. It's only logical. A more volatile asset will demand a higher option price to make up for the risk in said asset. Then you have the time to expiry. This is also generally positively correlated with price. As the longer that you have to expire the more time value you have of the option. The sensitivity of the price of the option to the rate of change in time is called “theta”. This time value also makes sense when you think about it. The longer you have till the expiry of the option, the longer the time period in which the option could either be in or out of the money. These are just some of the main factors that will impact on the price of an option and they are perhaps the most important for you to understand if you want to trade them.

Chapter 27 Trading Tips: Put Call Ratio

It’s time to explore how to use the option data to infer market trends and sentiment. Firstly I want to discuss the put call ratio. This is a measure of the ratio of the open interest or the volume of the puts, versus the calls. The open interest is a measure of the total amount of notional outstanding on a futures or options position. The volume is of course the total amount of options or futures that have been traded in a certain period. For example if we're talking about the open interest put call ratio, we're measuring the total notional outstanding value of all puts to that of the notional outstanding value of all calls. So what can we read from a put call ratio? Well it's able to give us a rough idea of general sentiment in the market. If there is more open interest outstanding for puts than calls, then that means there are larger bearish bets than bullish bets. Hence, a put call ratio of greater than one is viewed as more bearish than a ratio of less than one and vice versa. You can also view the put call ratio through time to get a feeling for how this broader market sentiment has changed. The ratio is slightly more than one when viewed with the volume metric and less than one when viewed with the open interest. I generally tend to use the open interest metric as this gives a more reliable indicator of outstanding trades than the total value of all the options being traded. So based on a put call ratio of 1.36, it means that the put option open interest is about 36% more than the corresponding call notional outstanding. On balance option market participants have more puts outstanding than they do calls. You may be wondering why is this relevant? Well, knowing how options traders are positioning themselves can give you a rough idea of which way they expect the spot market to go. And you should not really be fixated on the absolute number of the put call ratio but rather on how it moves. Whether it's increasing or decreasing, this can help give you a better sense of how that sentiment is changing. okay That's the put call ratio. Of course all this gives you is an overview of how the broader market is positioned. It doesn't really allow us to get a direct comparison in the pricing of puts or calls. This is where the option skew comes in.

Chapter 28 Trading Tips: Options Skew

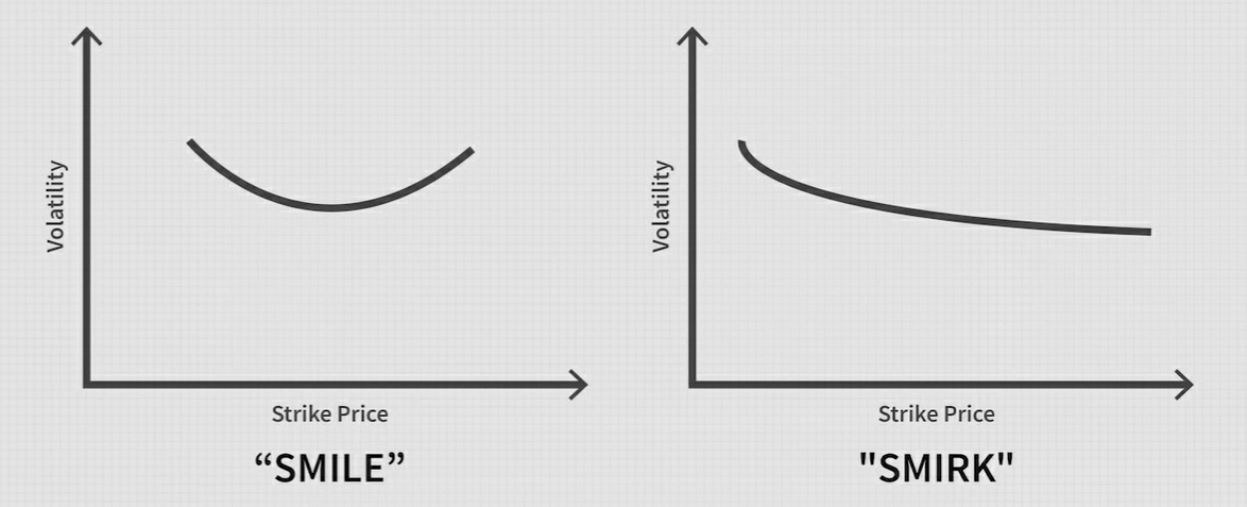
Option skew is a measure of the relative richness of the put, versus the call options expressed in terms of implied volatility. It's a measure of how much higher the implied volatility of put options with a specific delta are to call options with the same delta. All normalized by the at the money volatility. Here is the equation that's used to calculate the option 25 delta skew.

$$skew_T^{25d} = \frac{\sigma_{Put}^{25d}(T) - \sigma_{Call}^{25d}(T)}{\sigma^{atm}(T)}.$$

As you can see we're trying to get a measure of how much more implied volatility there is on the puts than the calls, relative to a standard measure of the implied volatility. Given the direct relationship between implied volatility and option premiums, you can also view this ratio as a rough measure of how much more the cost of puts are to calls. If we have two options with a similar sensitivity to the price of the underlying asset, how much more are people willing to pay to take on the puts; bearish versus to take on the bullish view with calls. Let's take a look at a quick example. Let's say that the 25 delta options skew is sitting at about 20%. This basically means that the implied volatility of a put option is about 20% greater than that of a call. We can also therefore infer that the price of similar put options is greater than the calls to a similar degree. This therefore means that option buyers are willing to pay more to buy put options, than they are to pay for calls with exactly the same parameters. You can view it as a more bearish sign. We can also say the opposite if the ratio is negative. Much like the case with the put call ratio, you can view the options skew over time. This is helpful as it allows you to get a sense of how the relative value and hence sentiment has changed recently. For example here you can see the 25 delta option skuw on skew.com for the past three months.



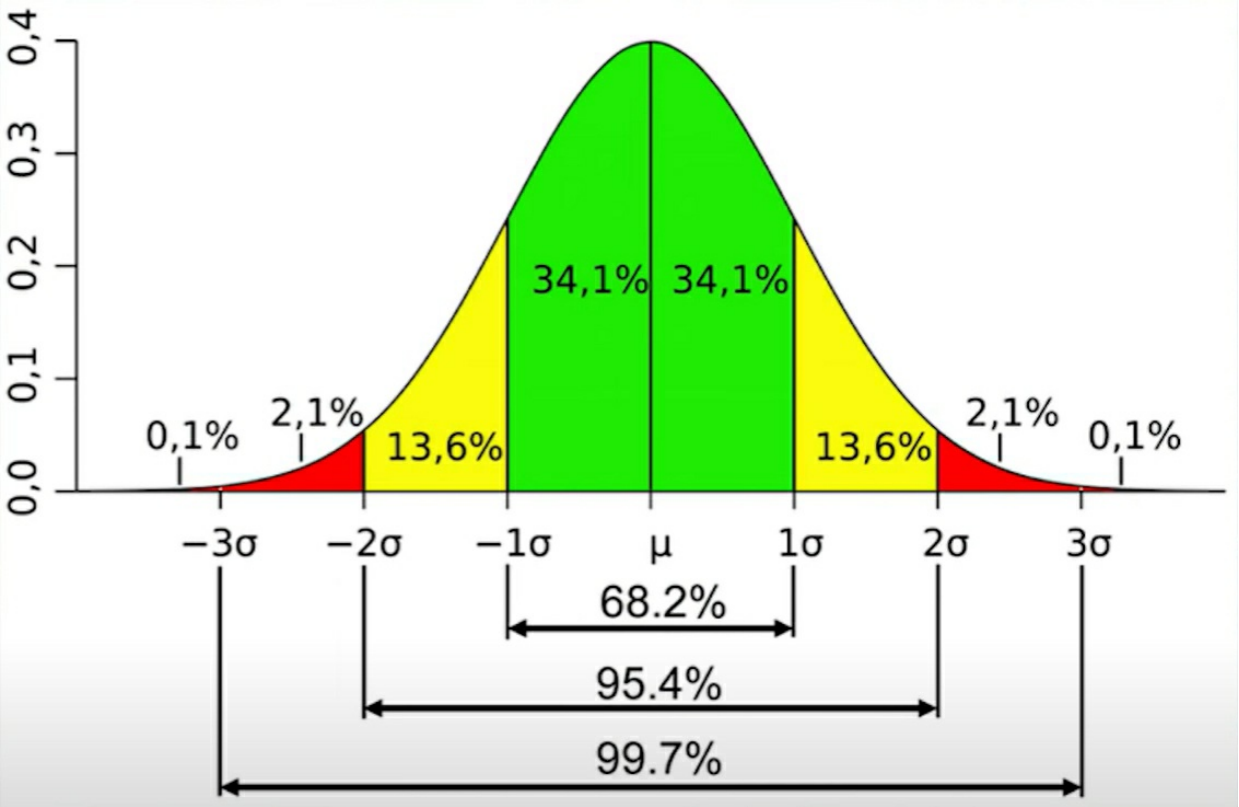
This is for a range of different option expiry times from one month all the way out to six months. If you only look at the three month option skew, you can see this is currently at negative 8.3%. This implies that the call options have a much higher implied volatility and hence the premium is greater than the puts. Generally a bullish sign. However if we take a look at how this has moved over the past three months you can see that it's been trending lower. What we can read from this is that market participants are paying more for calls than the puts. Not only that but the difference has increased over time which shows that their bullishness has too. If you take a look at the spot price of Bitcoin over the period you can see that it's quite well correlated with this fall in the skew. I should also point out that option skew is much broader than just this. You can compare the skew across the entire volatility term structure. You have something called the volatility smile which illustrates this well.



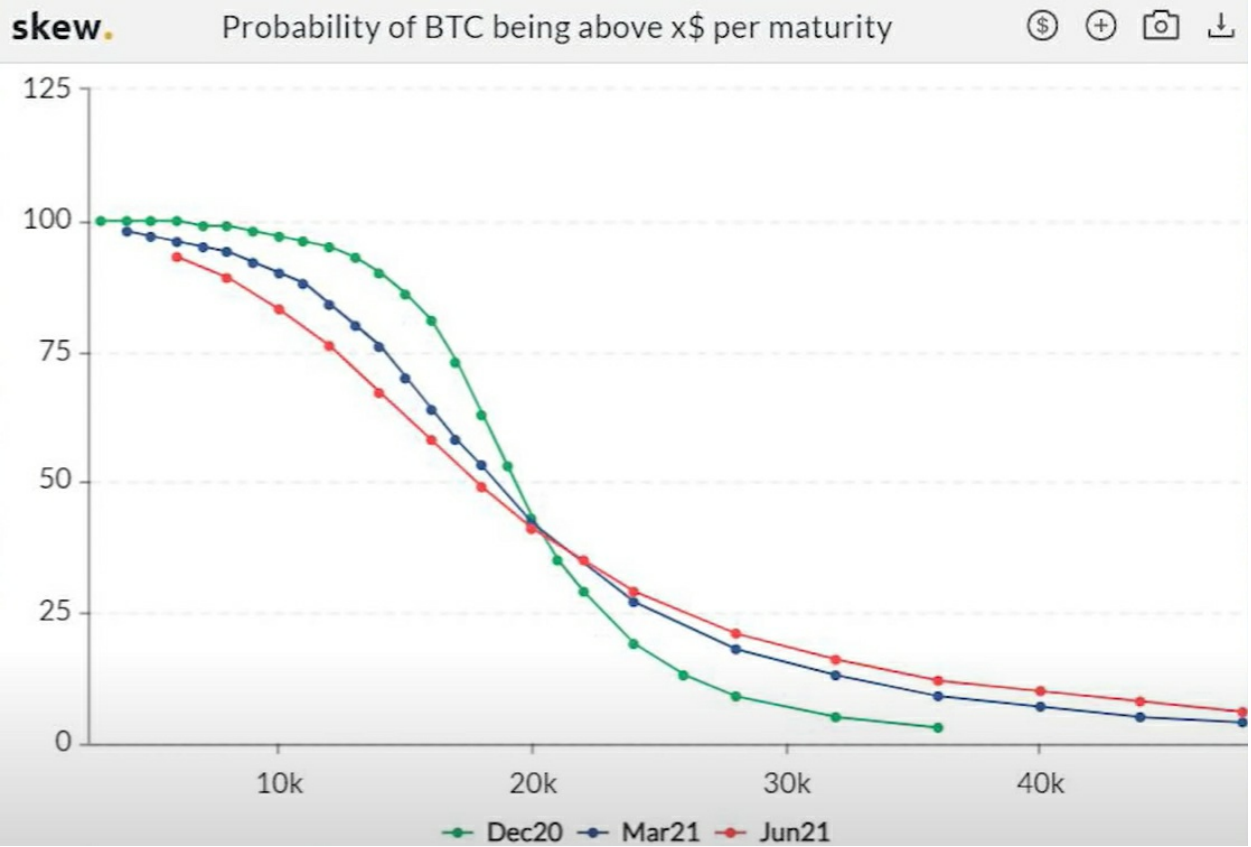
But that's an entirely different topic. All you need to know about option skew is that it's a helpful metric that I often use in order to gauge relative value and sentiment of an option. That's the skew. Now let’s take a look at another metric.

Chapter 29 Trading Tips: Market Parameters

It would be great if you could use the option price to calculate the probability of Bitcoin being above a certain price at maturity. Well, that's actually a reality thanks to the black skulls model. Assuming that you have the price of an option as well as all the other parameters in this equation, you can back out the potential price distribution of an asset on expiry. For those of you who did stats at University, you'll know all about probability density functions like the normal distribution.



If it's foreign to you, don't worry. All that we're doing here is using the market parameters of the options in order to back out the probability of it being above a chosen strike price. This is also something that you don't have to calculate yourself. skew.com has a graph that calculates this for us. Here you can see the probability distribution for a number of different option expiries. Let's take a look at the December 2020 option just to isolate it.



As you can see the probability of the price being above 22k on the 25th of December is about 28%. If we move down more we can see that the probability of being above 24k is about 19%. We can also take a look at the longer term options like the March and June 2021 ones to draw similar probabilities. So what can these probabilities tell you? Well, they can give you a rough idea of how likely certain future prices are based on pricing in the options market. I like to use these as they help to give me a sense of more realistic outcomes. In crypto we're quite desensitized to these parabolic price predictions, so much so that we can sometimes get caught up in the hype. However over on the options market, most of the participants taking out the largest positions are professional investors. I'm talking institutional funds and sophisticated market makers. The prices that they are willing to pay for option protection and exposure are likely to be a better benchmark for their real price predictions than what they claim on TV. Of course I should also caveat that you should not use this as any sort of bible. It's just a probability measure backed out from market data. It's a useful data point you can use in order to further inform your analysis. That is option price probabilities.

Chapter 30 Trading Tips: Options Expiry Dates

Something else that I really want to touch on now is the option expiry dates, more specifically the impact that this tends to have on the spot market. If you follow any sort of crypto news website or trading group, you'll sometimes hear reference to the “option expiry dates”. If there are a lot of options that are expiring on the date then this could be an indication that there's likely to be quite a lot of volatility on the day. So the important question here is; why and how can you judge the likely price direction on the expiry date? Let's start with that first one. There is volatility around these expiry dates because market participants are trying to adjust their positions for physical delivery of the underlying asset. Similarly, some market makers may need to adjust their hedge positions in the spot market, as they approach these pivotal moments in the option price. So what you have, is a situation in which option expiry events are having a direct impact on the underlying spot markets. When there's a large number of outstanding options, the impact on the spot market is likely to be that much greater. This is something that's been known in the equity markets for a number of years. These are sometimes termed the expiry weeks where volatility in the underlying share starts to pick up. However given the growth of Bitcoin options, we've also seen these instruments impacting the Bitcoin spot price. This usually tends to happen about two days before the actual expiry. Those participants that hold the option may either close out of their position or roll forward into new options on the expiry date. So we know that options expiry dates are usually dates of interest when it comes to price movements. But, is there a way to get a sense of which way it's likely to move? Well, there's no hard and fast way but you can get a vague idea by taking a deeper look into the options order books themselves. In this case, I'm going to be taking a look at the Deribit order books. They are the exchange with the most liquidity and functionality for retail traders. To logon to Deribit , please visit their website at https://www.deribit.com/

So let's take a look at some options that are about to expire soon. What we're looking for is to determine how much theoretical buying or selling pressure is likely to come in the spot market from the expiry from these calls or puts in the options market. Basically to get a rough back of the envelope put call ratio. Next, you can further the range of options to those that are relatively close to the money level. Here you might choose an acceptable range for

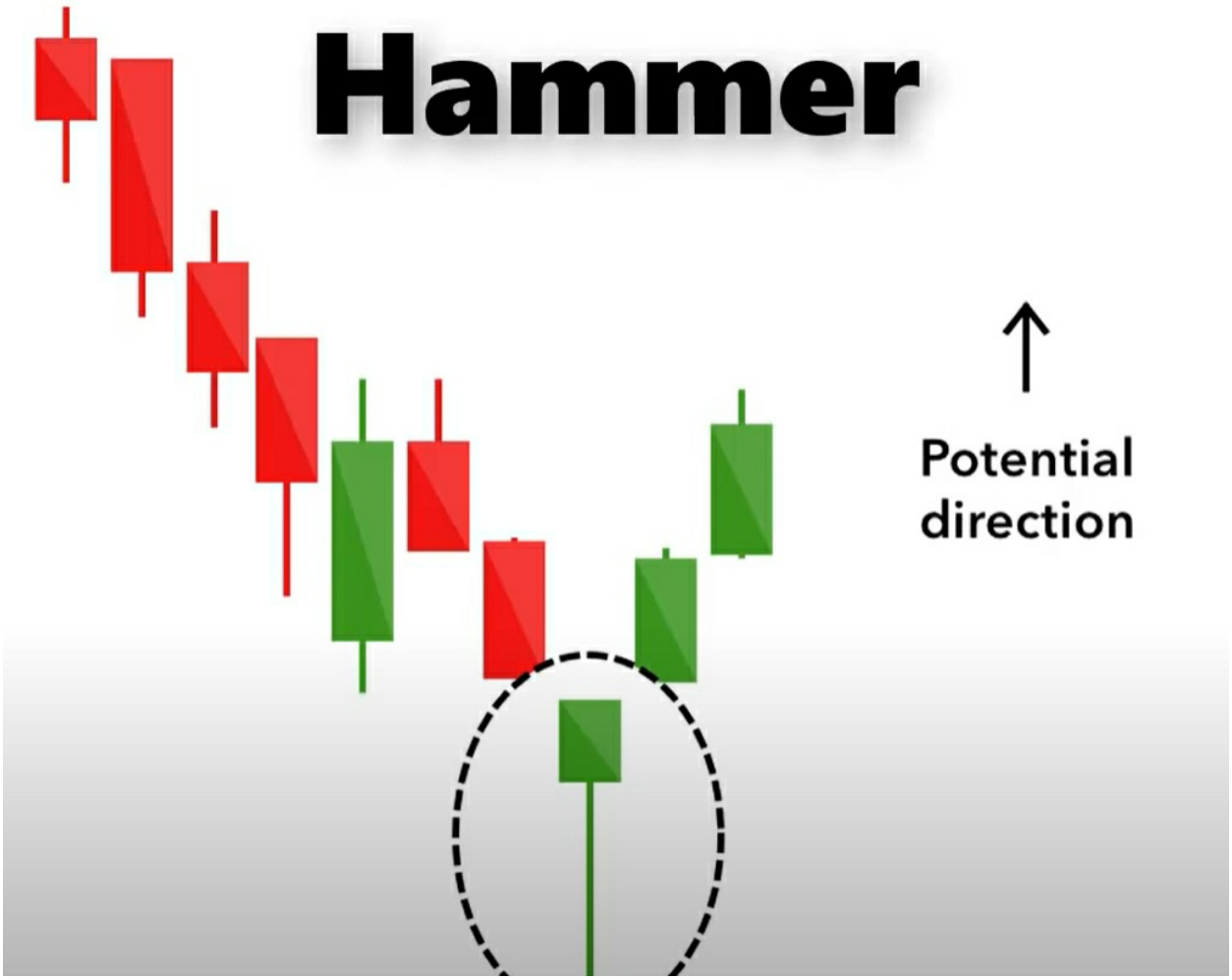
both. In my case I'm of the view that on the 21th of December Bitcoin is likely to be within the 21K to 23.5K level. Hence I take a look at all the options that fall into this range. Now I want to try and determine the total outstanding notional or open interest on the call and then the put side. With these option expirations, the total open interest on the calls is about 4200 Bitcoin. Whereas on the put side the total notional outstanding is about 1770 Bitcoin. So, what this shows us is that as we roll forward towards the December 21st expiry date, there are a lot more cool positions in the market; almost 2.4 times more. So theoretically, this means that there is more chance of there being buying pressure in the spot market as we head into the expiry than selling pressure. A more bullishly positioned market. Of course I should caveat that at the time of doing this analysis there was still about two weeks to expiry. A lot can change closer to the expiry date and as I mentioned before in the Bitcoin markets the impact on spot markets of the open expiry only tends to be felt two or three days before. So, if you're going to be using this analysis method, I would encourage you to re-examine the relative open interest balance as we get closer to expiry time. You should also note that this is not a science. There are many other factors that can swing the price on expiry. Let's not forget that you also have the impact of the futures markets as well as large whale orders going through on the spot market. But, it is a handy guide that I use from time to time. The truth is that the particulars of this relationship between the derivatives and spot markets are fascinated. There may be some things here that are hard to grasp and that's totally okay. The truth is that most people who trade options don't really focus too much on the underlying equations. They're more concerned about overarching concepts. Knowing exactly how the 25 delta skew is calculated is of way lesser importance than understanding what it means. What does it show about how the market is positioned and how you can use that information in your broader research toolbox. Similarly, having a rough idea of what price distributions are in the future, can help you adjust your expectations. You can get a rough idea of price probabilities from the options markets and it always helps to keep an eye on option expiry dates. Even if you don't try to conclude a particular price direction, it has been shown these dates cause spot market volatility. By having these dates pinned in your calendar, you're better prepared to deal with any potential volatility that could result. There's nothing worse than being caught off guard by a large price gap; be it up or down. So I hope that you can find some of these indicators and tools helpful in your

price analysis. They can be that much more interesting when actually used to trade options themselves.

Chapter 31 Bullish Candlestick Patterns

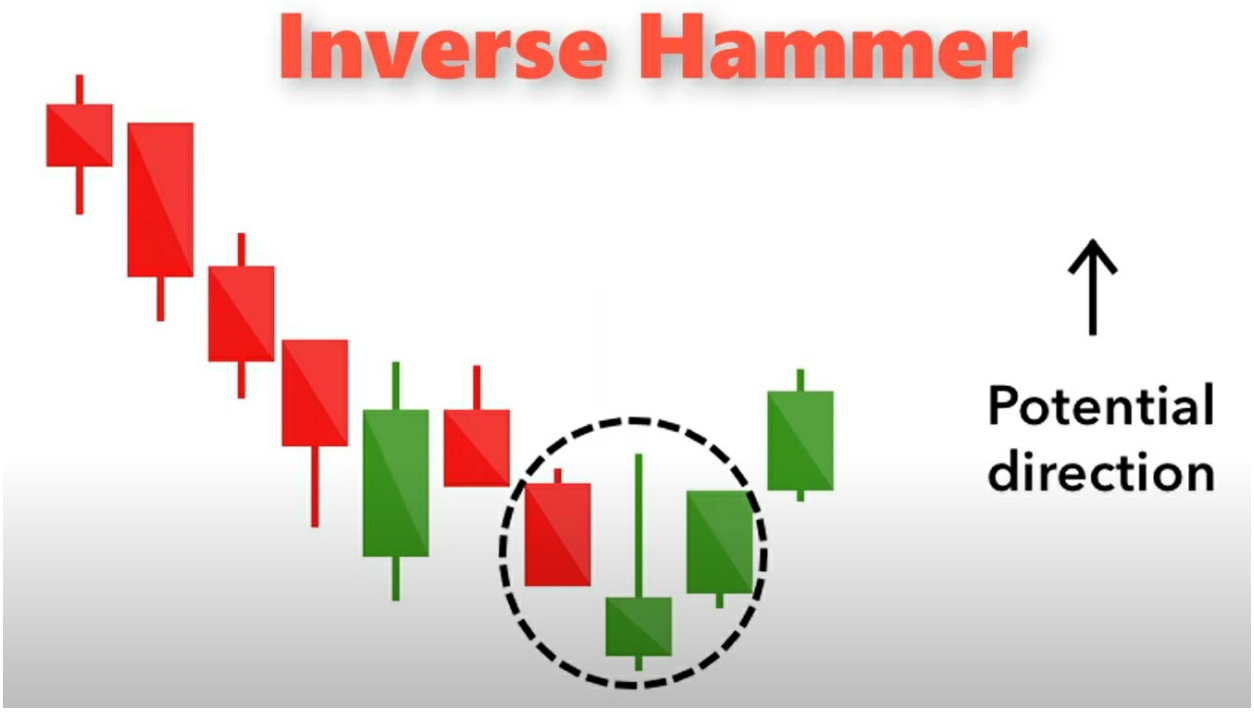
In this chapter you will learn about candlestick patterns. What is a candlestick? Well, a candlestick is a way of displaying information about an assets price movement. Candlestick charts are one of the most popular components of technical analysis, enabling traders to interpret price information quickly and from just a few price bars. This chapter will focus on a daily chart where in each candlestick details a single day's trading. It has three basic features. The body which represents the open to close range. The wick or shadow that indicates the intraday high and low. The color, which reveals the direction of market movement. A green or white body indicates a price increase, while a red or black body shows a price decrease. Over time individual candlesticks form patterns that traders can use to recognize major support and resistance levels. There are a great many candlestick patterns that indicate an opportunity within a market. Some provide insight into the balance between buying and selling pressures, while others identify continuation patterns or market and decision. Before you start trading, it's important to familiarize yourself with the basics of candlestick patterns and how they can inform your decisions. Bullish patterns may form after a market downtrend and signal a reversal of price movement. They are an indicator for traders to consider opening a long position to profit from any upward trajectory.

Hammer



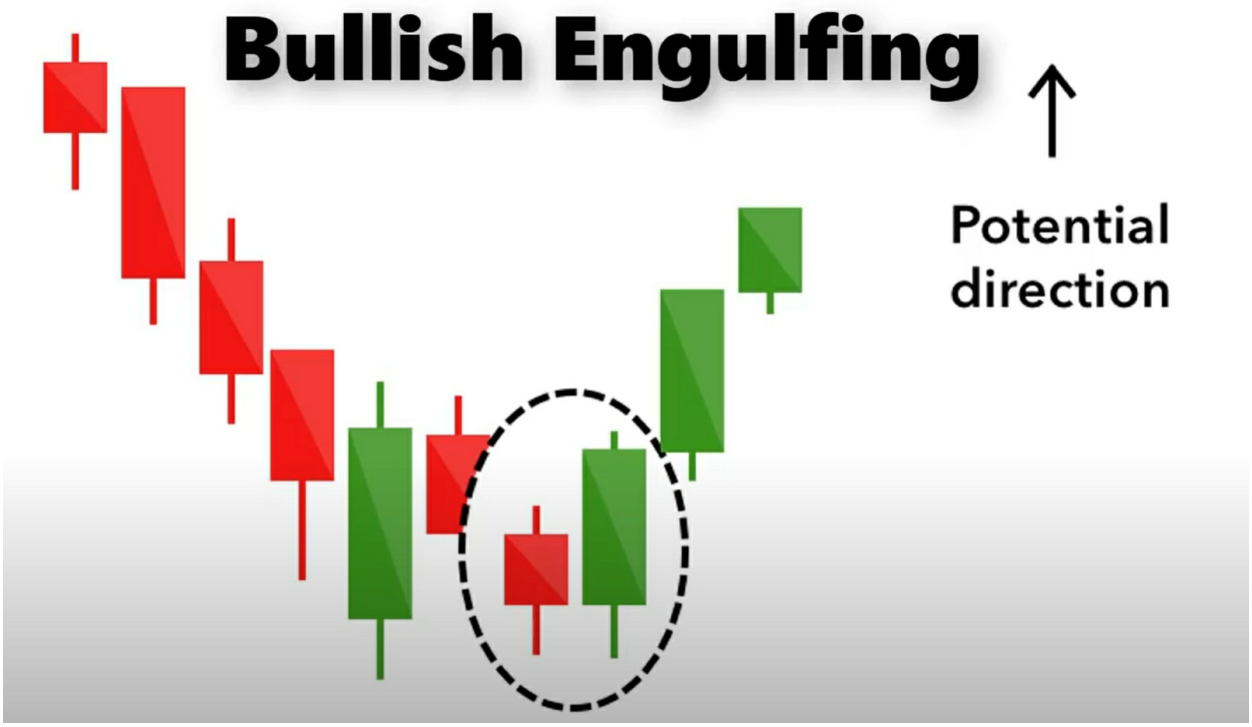
The hammer candlestick pattern is formed of a short body with a long lower wig and is found at the bottom of a downward trend. A hammer shows that although there were selling pressures during the day, ultimately a strong buying pressure drove the price back up. The color of the body can vary, but green hammers indicate a stronger bull market than red hammers.

Inverse hammer



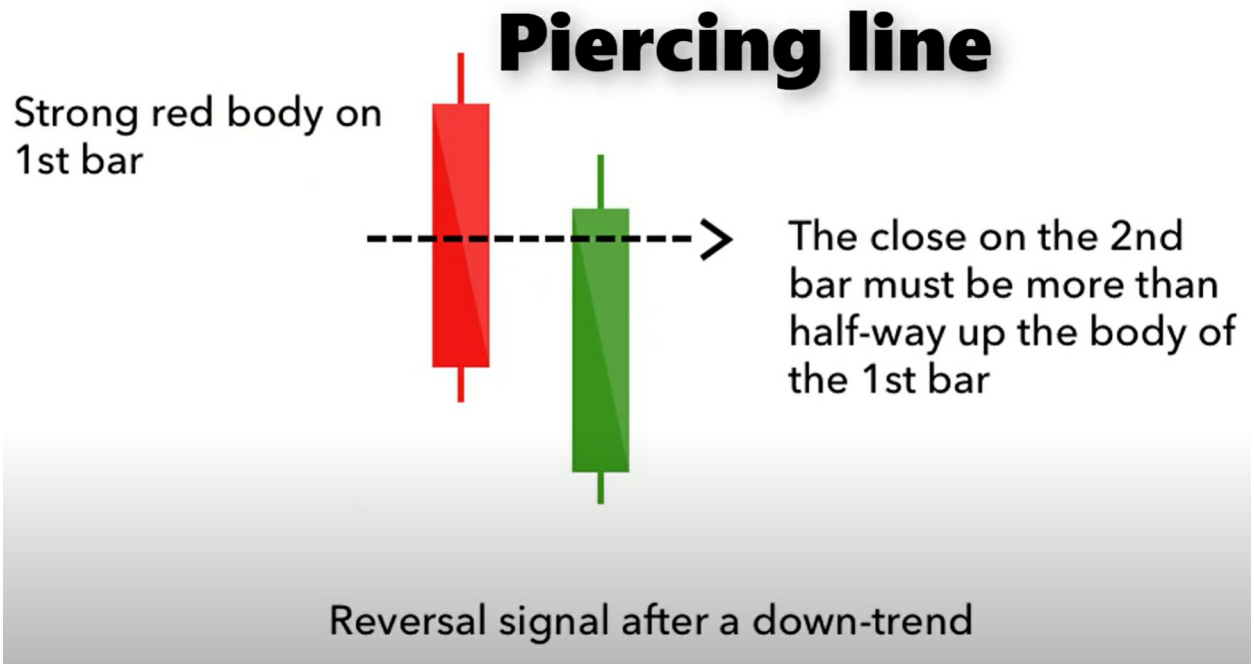
A similarly bullish pattern is the inverted hammer. The only difference being that the upper wick is long, while the lower wick is short. It indicates a buying pressure followed by a selling pressure that was not strong enough to drive the market price down. The inverse hammer suggests that buyers will soon have control of the market.

Bullish engulfing



The bullish engulfing pattern is formed of two candlesticks. The first candle is a short red body that is completely engulfed by a larger green candle. Though the second day opens lower than the first, the bullish market pushes the price up. Culminating in an obvious win for buyers.

Piercing line



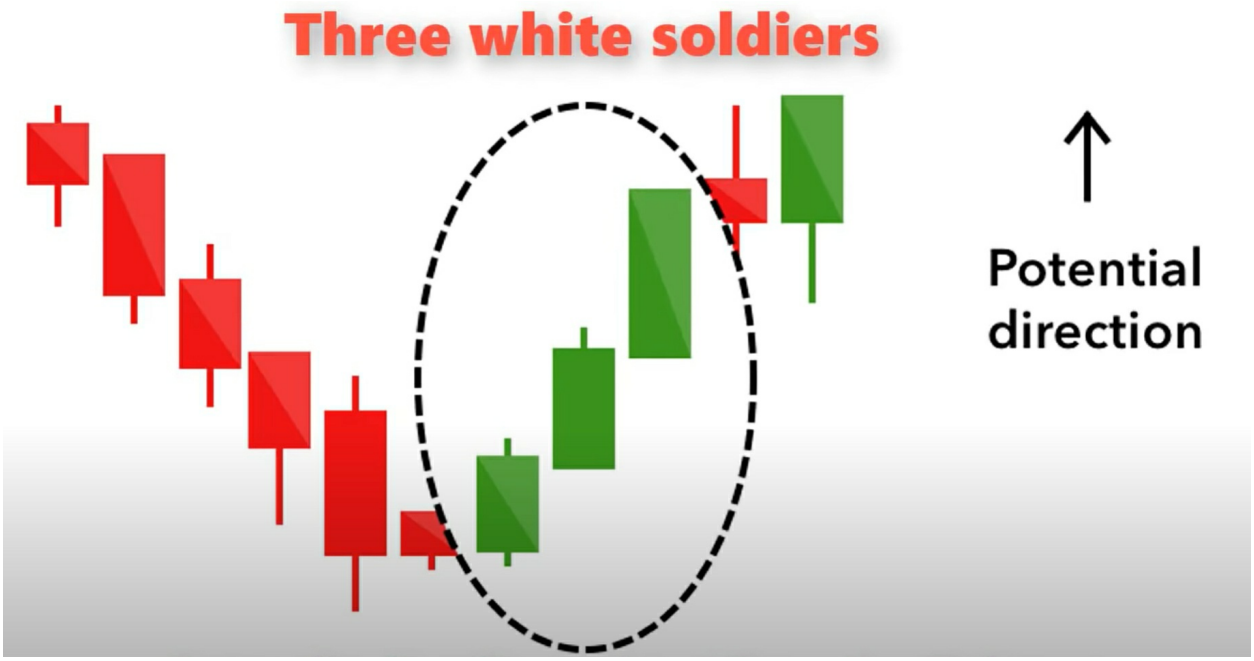
The piercing line is also a two stick pattern made up of a long red candle, followed by a long green candle. There is usually a significant gap down between the first candlesticks closing price and the green candlesticks opening. It indicates a strong buying pressure as the price is pushed up to or above the mid price of the previous day.

Morning Star



The Morningstar candlestick pattern is considered a sign of hope and a bleak market downtrend. It is a three stick pattern one short bodied candle between a long red and a long green. Traditionally, the star will have no overlap with the longer bodies as the market gaps both on open and closed. It signals that the selling pressure of the first day is subsiding and a bull market is on the horizon.

Three white soldiers

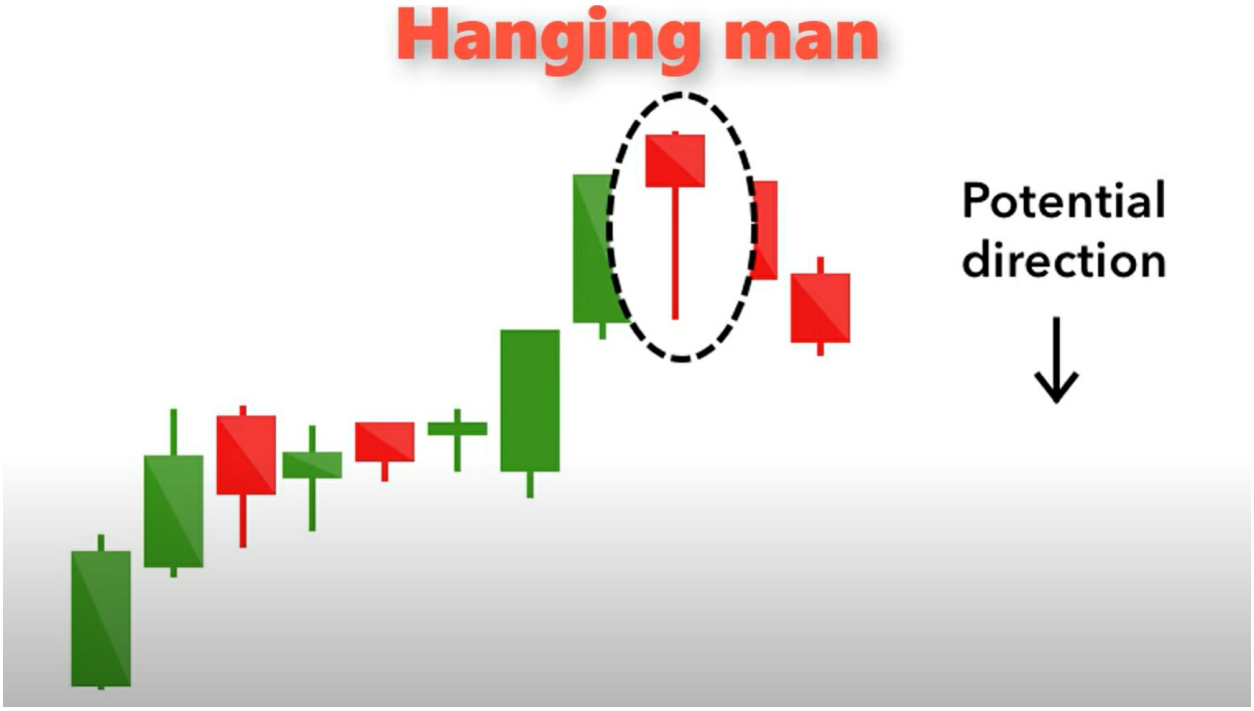


The three white soldiers pattern occurs over three days. It consists of consecutive long green or white candles with small wicks which open and close progressively higher than the previous day. It is a very strong bullish signal that occurs after a downtrend and shows a steady advance of buying pressure.

Chapter 32 Bearish Candlestick Patterns

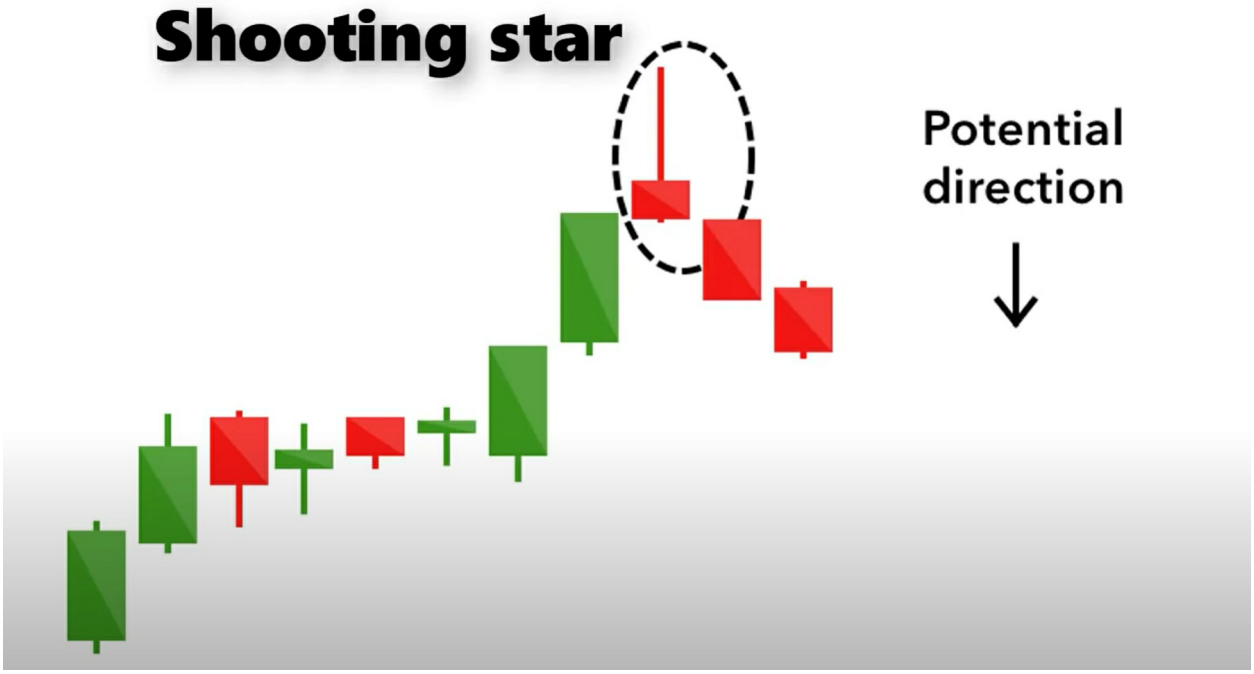
Bearish candlestick patterns bearish candlestick patterns usually form after an uptrend and signal a point of resistance. Heavy pessimism about the market price often causes traders to close their long positions and open a short position to take advantage of the falling price.

Hanging man



The hanging man is the bearish equivalent of a hammer. It has the same shape but forms at the end of an uptrend. It indicates that there was a significant sell-off during the day, but that buyers were able to push the price up again. The large sell-off is often seen as an indication that the Bulls are losing control of the market.

Shooting star



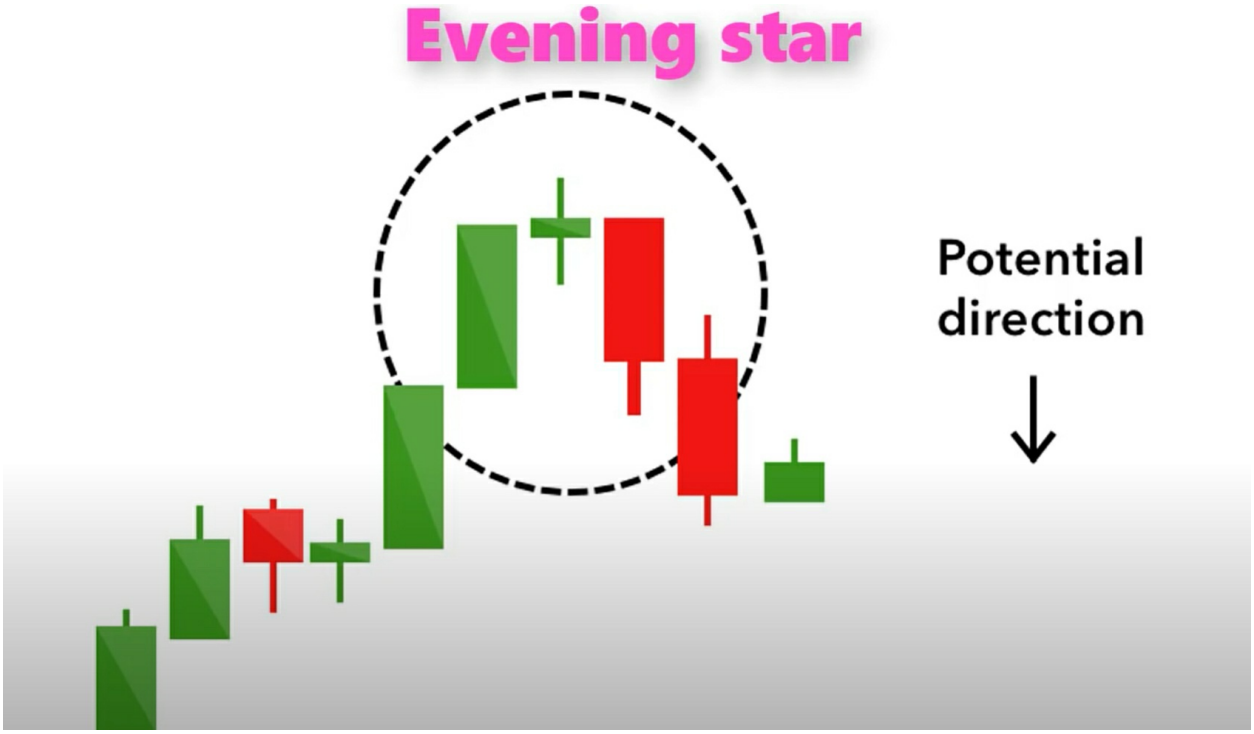
The shooting star is the same shape as the inverted hammer, but is formed in an uptrend. It has a small lower body and a long upper wick. Usually the market will gap slightly higher on opening and rally to an intraday high before closing at a price just above the open. Like a star falling to the ground.

Bearish engulfing



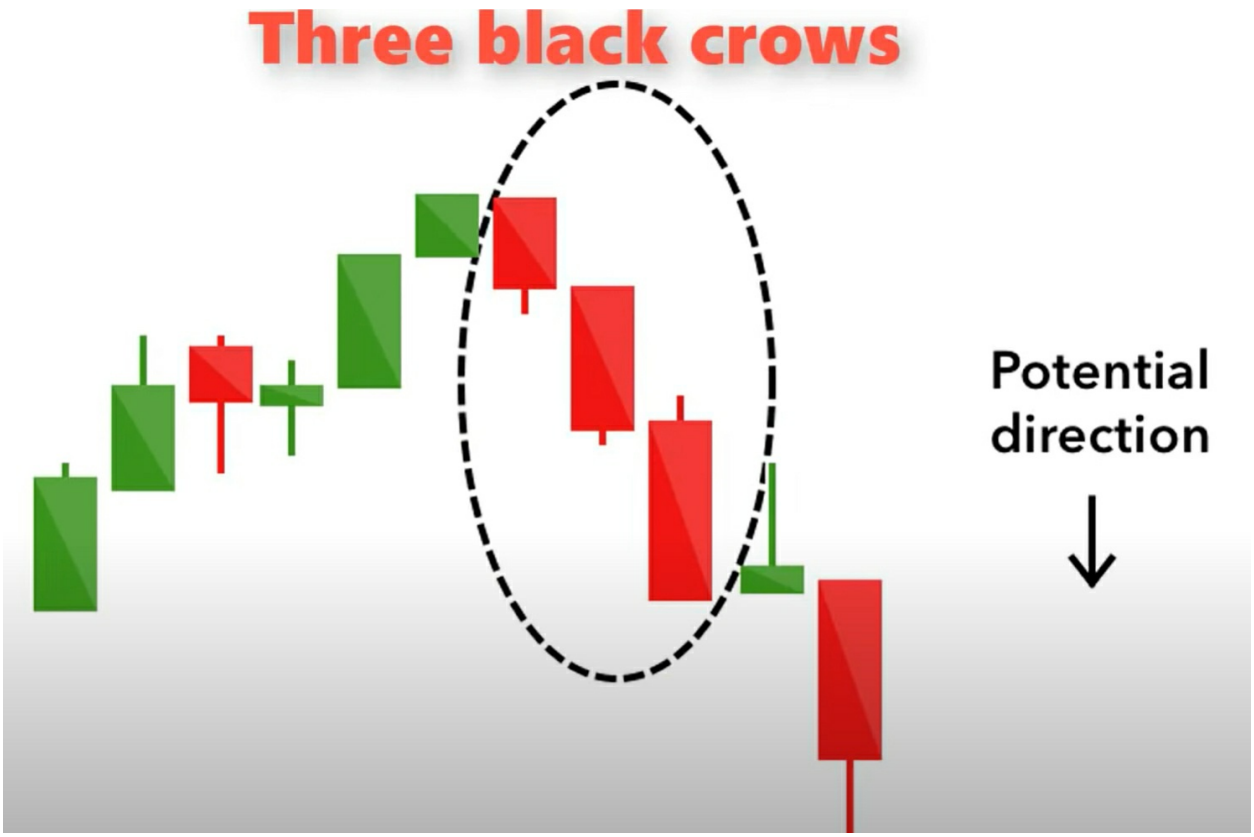
A bearish engulfing pattern occurs at the end of an uptrend. The first candle has a small green body that is engulfed by a subsequent long red candle. It signifies a peak or slowdown of price movement and is a sign of an impending market downturn. The lower the second candle goes the more significant the trend is likely to be.

Evening star



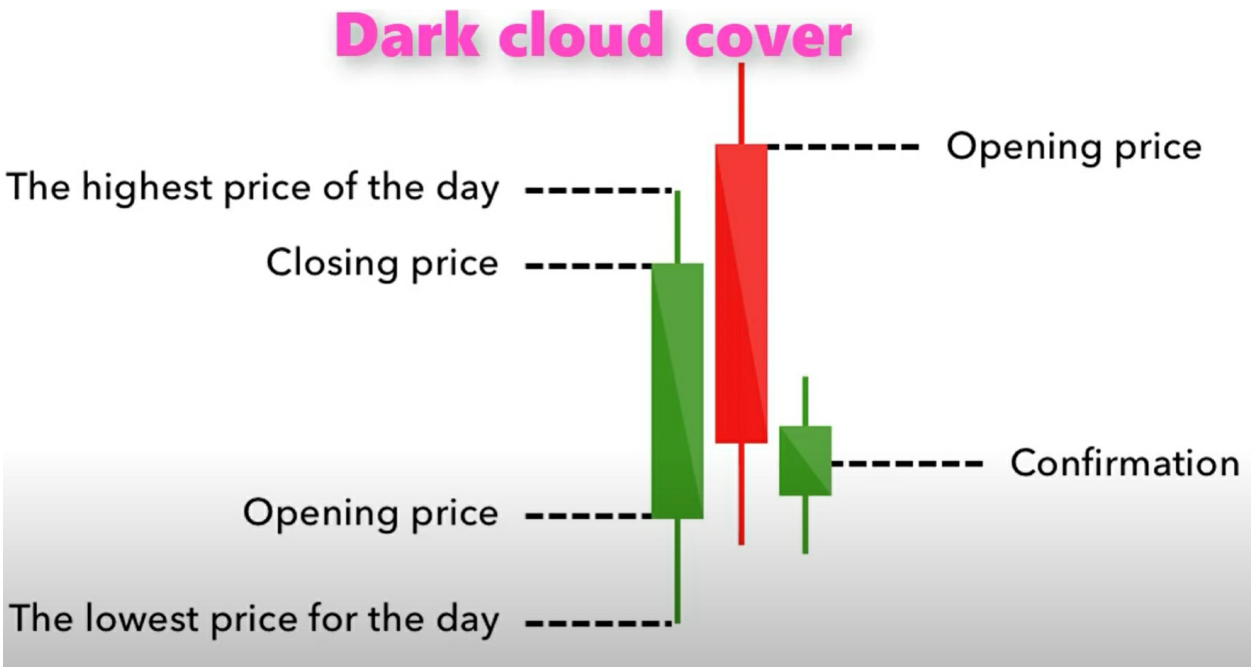
The evening star is a three candlestick pattern that is the equivalent of the bullish Morningstar. It is formed of a short candle sandwiched between a long green candle and a large red candlestick. It indicates the reversal of an uptrend and is particularly strong when the third candlestick erases the gains of the first candle.

Three black crows



The three black crows candlestick pattern comprises of three consecutive long red candles with short or non-existent wicks. Each session opens at a similar price to the previous day, but selling pressures push the price lower and lower with each close. Traders interpret this pattern as the start of a bearish downtrend as the sellers have overtaken the buyers during three successive trading days.

Dark cloud cover

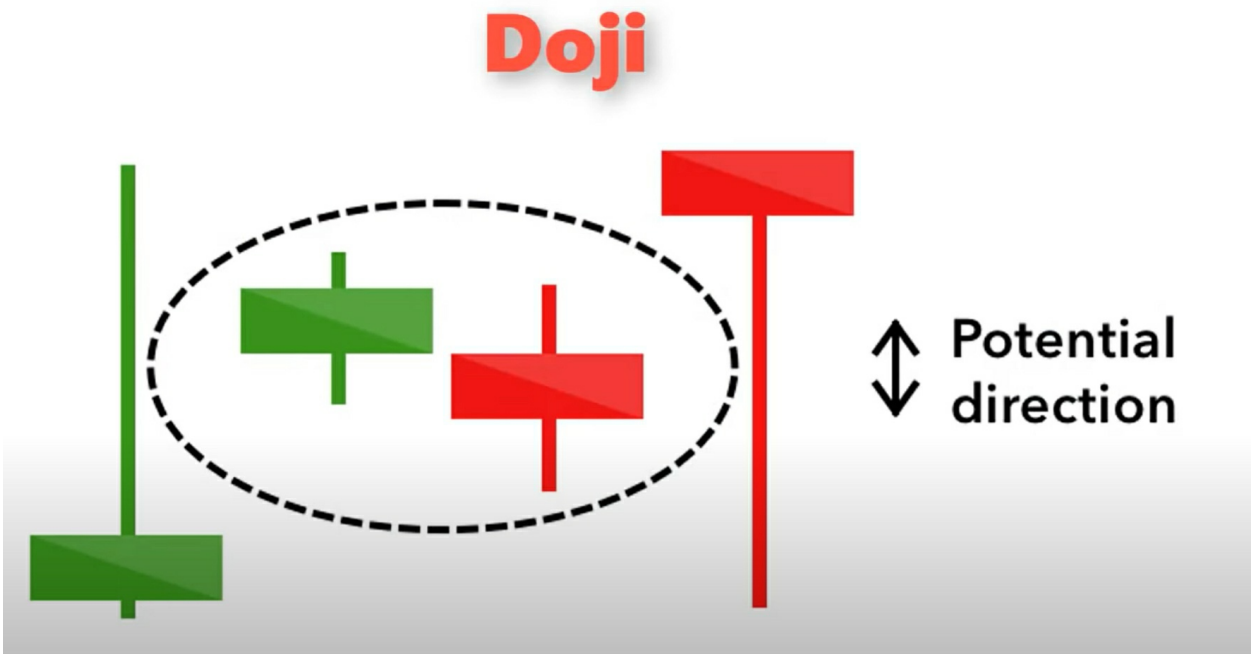


The dark cloud cover candlestick pattern indicates a bearish reversal. A black cloud over the previous day's optimism. It comprises two candlesticks. A red candlestick which opens above the previous green body and closes below its midpoint. It signals that the Bears have taken over the session, pushing the price sharply lower. If the wicks of the candles are short, it suggests that the downtrend was extremely decisive.

Chapter 33 Continuation Candlestick Patterns

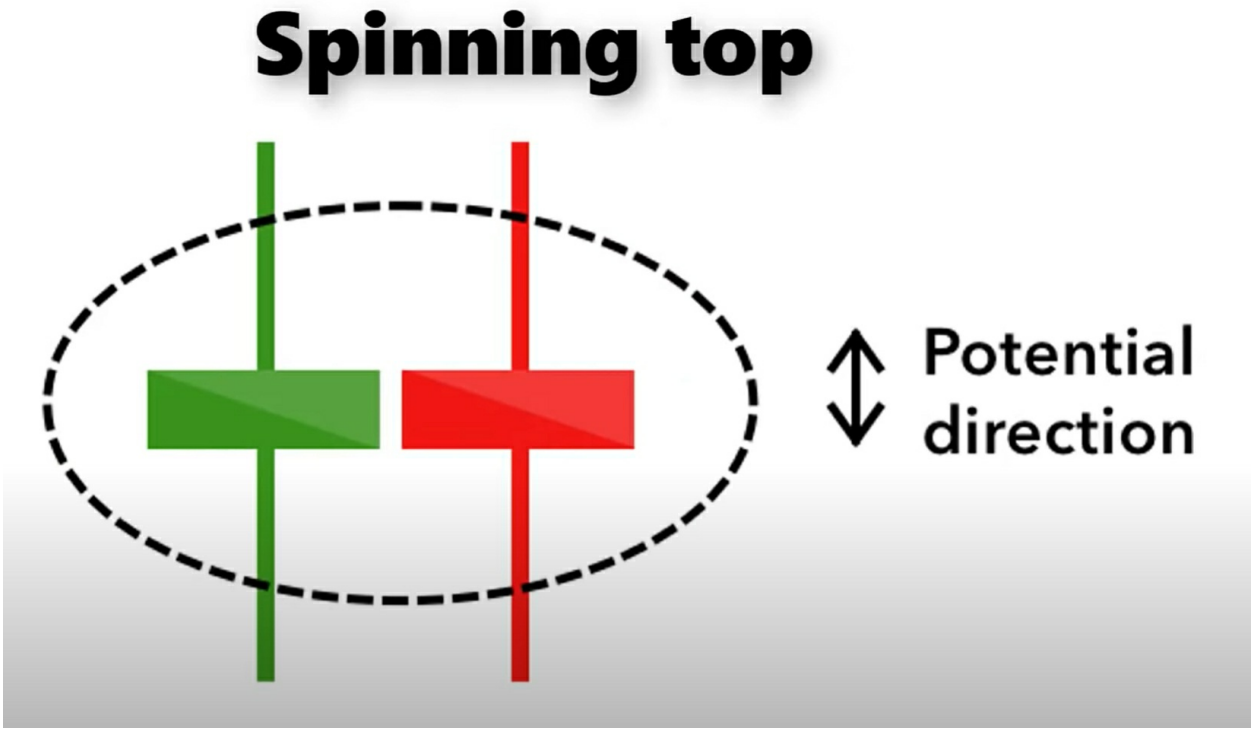
For continuation candlestick patterns, if a candlestick pattern doesn't indicate a change in market direction it is what is known as a continuation pattern. These can help traders to identify a period of rest in the market when there is market indecision or neutral price movement.

Doji



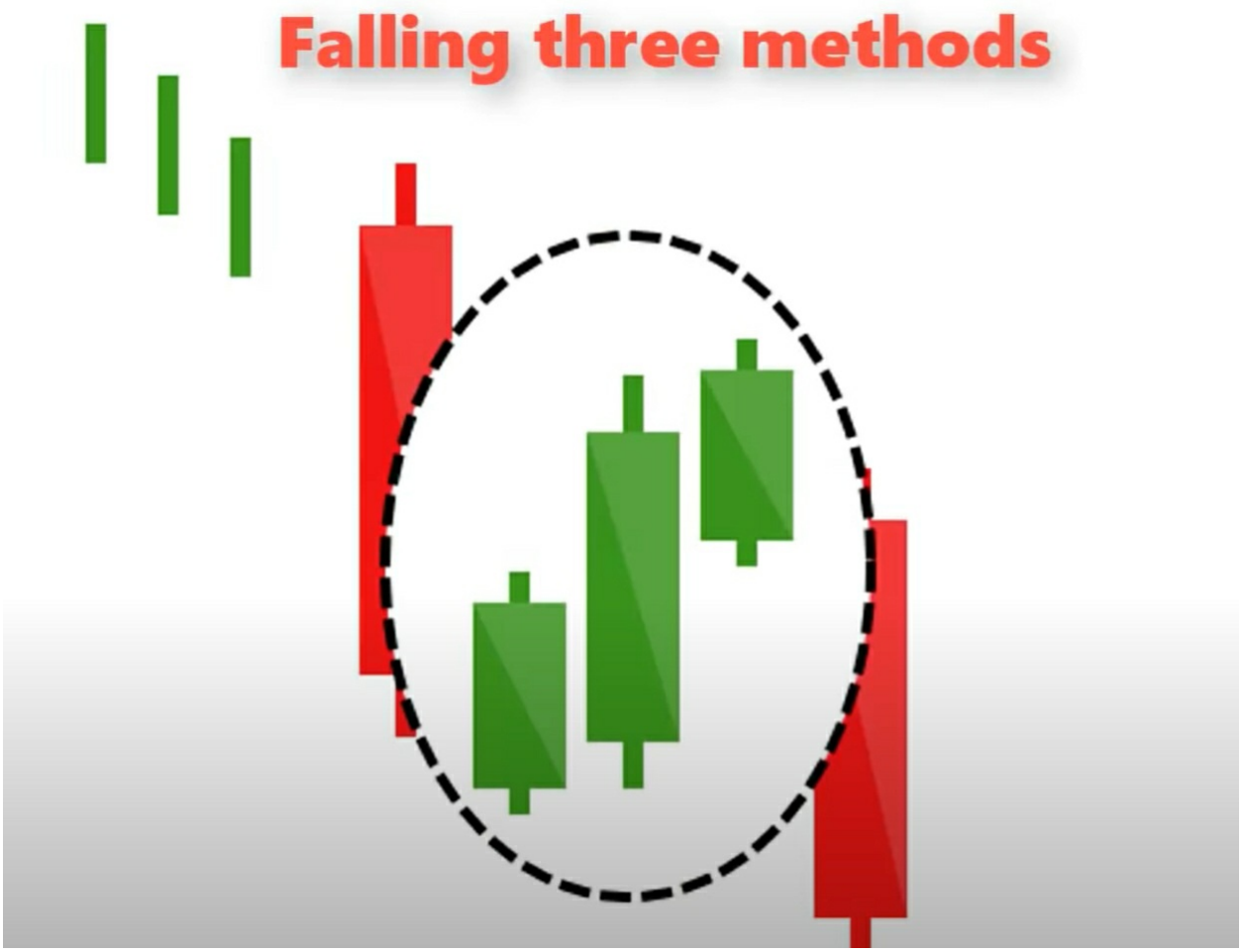
When a markets open and close are almost at the same price point, the candlestick resembles a cross or plus sign. Traders should look out for a short to non-existent body with wicks of varying lengths. This doji's pattern conveys a struggle between buyers and sellers that results in no net gain for either side. Alone a doji is neutral signal but it can be found in reversal patterns such as the bullish Morningstar in bearish evening star.

Spinning top



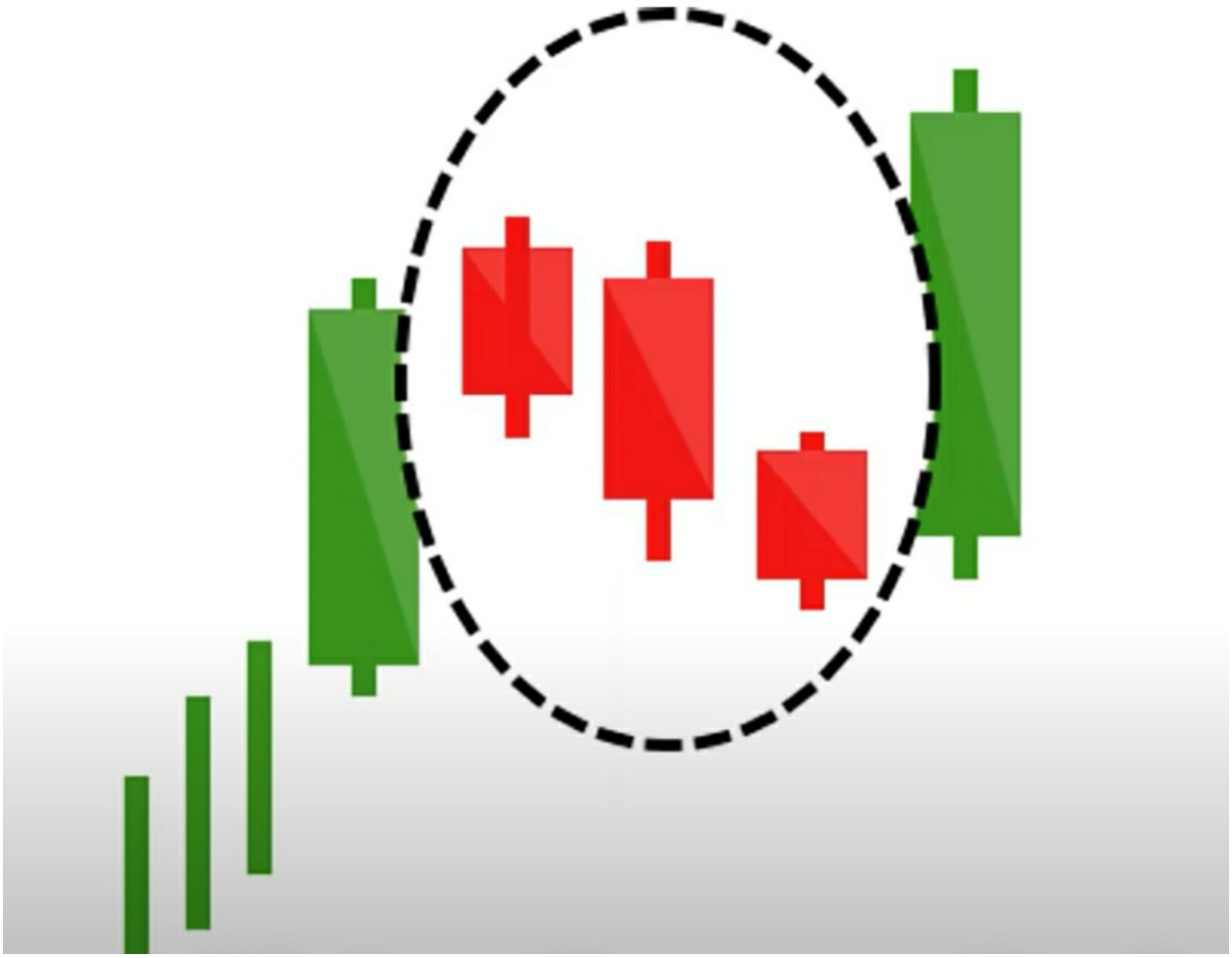
The spinning top candlestick pattern has a short body centered between wicks of equal length. The pattern indicates indecision in the market, resulting in no meaningful change in price. The Bulls sent the price higher while the Bears pushed it low again. Spinning tops are often interpreted as a period of consolidation, or rest, following a significant uptrend or downtrend. On its own the spinning top is a relatively benign signal, but they can be interpreted as a sign of things to come as it signifies that the current market pressure is losing control.

Falling three methods



Three methods formation patterns are used to predict the continuation of a current trend; be it bearish or bullish. The bearish pattern is called the falling three methods; it is formed of a long red body followed by three small green bodies and another red body. The green candles are all contained within the range of the bearish bodies. It shows traders that the Bulls do not have enough strength to reverse the trend.

Rising three methods



The opposite is true for the bullish pattern called the rising three methods candlestick pattern. It comprises of three short red sandwiched within the range of two long greens. The pattern shows traders that despite some selling pressure, buyers are retaining control of the market.

The best way to learn to read candlestick patterns is to practice entering and exiting trades from the signals they give. If you don't feel ready to trade on live markets, you can develop your skills in a risk-free environment by opening an test account. When using any candlestick pattern, it is important to remember that although they are great for quickly predicting trends, they should be used alongside other forms of technical analysis to confirm the overall trend.

Chapter 34 Trading Tips for Success

In this chapter I will reveal the secret to trading success and it's probably not what you're expecting. To become a successful trader he needs to know this. Around 90% of all traders lose money, so only 10% manage to be consistently profitable. But what is it that these successful 10% do different than the failing 90%? Well, first let's take a look at the typical trader of the 90% losing traders. Most people that are in this losing category are doing the following. They're somehow hear about trading and they believe that is all about the fancy lifestyle of a successful trader like easy money, work from anywhere in the World, expensive cars and the list goes on. They filled with motivation and greed. These people then sign up to the best broker that they probably found through some misleading commercial. Some people even watch one or two random YouTube trading videos before depositing their money to the broker platform. After signing up they usually start buying random stocks due to random reasons. To their surprise, the stocks rarely shoot up in price more from the not they exit their positions with a loss. Before they know it, they become part of the 90% losing trader group. Clearly not all losing traders go through these stages but a big deal of them do. I'm not saying this to mock the losing traders. I'm simply trying to compare losing to winning traders. My point is that consistently profitable traders actually know what they're doing. They usually have years of experience laid out and test the trading system. Furthermore, profitable traders have a trading plan and before they enter any trade, they know what they will do for changes in their position. In other words trading isn't easy. If it would be easy everyone would be doing it. Let's compare trading to other professions now. Would you try to fly an airplane without any guidance, education and practice? If you would, it would probably end through quite bad. Or would you try to perform a heart surgery without going to med school without any practice experience or education? Chances are high that you answered no to the previous two questions. To become a surgeon or pilot or anything else you normally need to go through years of training studying and practice. Why should this be different for trading? Just like no one is born as a perfect heart surgeon, no one is born as a perfect profitable trader. You need to study, practice and work your way up. If you try to fly an airplane without any education you would probably crash and blow up. The

same goes for your trading account. Trading without any education, usually leads to you blowing up your account. Don't make the mistake and risk your hard earned money without educating yourself before. The key takeaway here is that you need education to become a profitable trader. The next question is; do you need paid education or can you learn how to trade for free? Both free and paid trading education have their advantages and disadvantages. First of all let’s take a look at the advantages of paid education. One major advantage of paid education is the motivational aspect. People tend to be more committed to things that they actually paid for. This is because they feel like something is on the line. A further advantage is the focus on one strategy. Most good paid trading courses focus on one strategy and teach you everything important for that particular strategy. Most paid education is therefore more specific and relevant than free education. In other words, many paid trading courses of higher quality than free courses. In addition to that, premium costs often come with personal support. Let's move on to the advantages of free education. The most obvious Pro is the fact that it's free. If the free education is bad, it doesn't matter because you didn't pay anything for it. Next up other disadvantages of the paid trading courses. First of all one disadvantage is the fact that it costs money, therefore something is on the line. If the education is poor quality, you wasted your money. Some of these so-called trading courses are scams so be careful. Another major disadvantage is the lack of transparency. Many trading educators earn all the money from their trading education and nothing from that trading. Just because someone tells you he is a massively profitable trader, does not mean that he actually is. The last but not least, the fact that paid education is very specific is also a disadvantage. It is always good to have a wide general knowledge. Most paid courses focus on their strategies and ignore the bigger picture. Lastly, we have the cons of the free education. Often free trading courses can be less thorough therefore it can generally be hard to find very good and in-depth free trading courses. Thus free education requires a little more work. Before we move on I just want to say that these pros and cons are generalizations. Not all of the advantages and disadvantages applied to all free and paid trading courses. Obviously there are exceptions. As you can see both free and paid trading courses have their advantages and disadvantages. It can be quite hard to pick one over the other. In my opinion it's best to combine free and paid trading education. This will let you take advantage of the pros of both free and paid education. I recommend starting with free

education. All basic trading concepts can be learned from free education. I do not recommend spending any substantial amount of money just to learn the basics. You should be able to learn very important basic concepts such as asset types, basic charting, risk management and so on from free education. After doing this, I suggest asking some questions. Are you still interested in trading? Are you still willing to put in more work to learn how to trade? If yes, what trading style fits you? Aspects to consider here are starting capital, time, risk tolerance and so on. As you learned about different asset types, you should have an idea of what asset types fits you. Next, I recommend looking at paid training courses. You should already have a fundamental understanding of trading and the markets in general. Ideally you should also have a preferred asset type like options, stocks, cryptocurrency. When trying to find a good trading course, you should do some research. Try to find a course that fits you, your starting capital, your the time and so on. Look for proven track records and success stories. Generally, if something sounds too good to be true it probably is. Please don't skip the research part. There are countless scams out there so be careful. This is one of multiple ways to learn how to trade but you can do it differently as well. For example you could just pay for everything if you have more than enough money but remember; only the very last step is trading. Don't risk your hard earned money before you actually know what you're doing. Otherwise you will just end up like 90% of all traders. Before starting to trade real money, you should have a good understanding of trading at the markets. You should also have a proven profitable system a concrete trading plan and you should have had loads of education. Even after you start Trading, you should try to continue to learn more. Never follow random trade alerts. Never rely on one or two random indicators. Never listen to seemingly magic trading software. Just do it the right way. Educate yourself and learn how to trade. Remember, if it would be easy everyone would be doing it. The last piece of the puzzle is trading like is your profession and not as a hobby. The secret to trading success is the same as the secret to success in general. It's hard work, experience, education, taking action and practice.

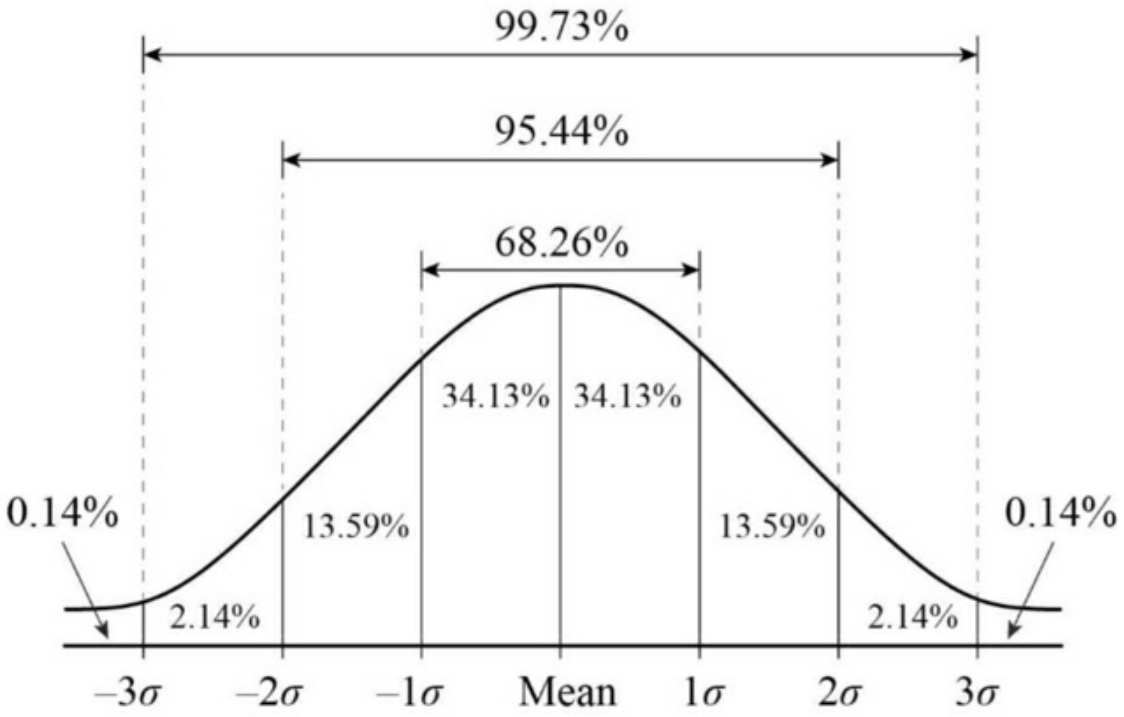
Chapter 35 What is Implied Volatility

In this chapter you will learn everything you need to know about implied volatility, what implied volatility rank is and why it matters. First of all, what is implied volatility? Well, implied volatility can be derived from options pricing models such as the Black Scholes options pricing model. It can be thought of as they expected likelihood of certain price changes in the underlying asset. But what does that mean? Well, to understand this let's break down what goes into an options price. The black Scholes formula uses the following variables to calculate an options price. The underlying price, the strike price, the expiration date, the risk-free rate and implied volatility. The first two factors are quite obvious because they determine the intrinsic value of an option. The expiration date also makes a lot of sense as more time to expiration gives your position, more time to work. Thus time to expiration should definitely affect the price of an option. The risk-free rate only has a very small effect on an options price and doesn't change significantly over short periods of time therefore it can be ignored for now. Last but not least the volatility of the underlying asset should also affect the options price because more volatile assets tend to give an options trader more opportunity to profit from price swings, whereas on volatile assets have limited trading opportunities. For instance, a far out of the money option is far more likely to become in the money if the underlying asset is very volatile then if it's not. Therefore volatility is one of the factors used to calculate a theoretical options price. However, it's fairly easy to observe and measure the underlying price, strike price and time to expiration. But it's not as straightforward to measure the volatility of the security, especially not the future volatility. That's why models such as the Black Scholes Model use a formula to determine the implied volatility from the options price instead of the options price from the implied volatility. An options price can be observed in the markets together with all the other factors except for volatility. From all this you can calculate a theoretical volatility value. This volatility value is implied from the options price, therefore it's called implied volatility. So when you hear in some financial news that options traders are expecting upcoming volatility, what they're really saying is that the volatility implied by the current option prices, where the implied volatility is relatively high. Note that implied volatility is not the same as historical volatility. Historical volatility is the past actual

volatility and it does not affect the options price, whereas implied volatility does. Furthermore, implied volatility is a purely theoretical value therefore implied volatility values often differ from the actual volatility values over certain time periods. Hopefully this helps you understand what implied volatility is.

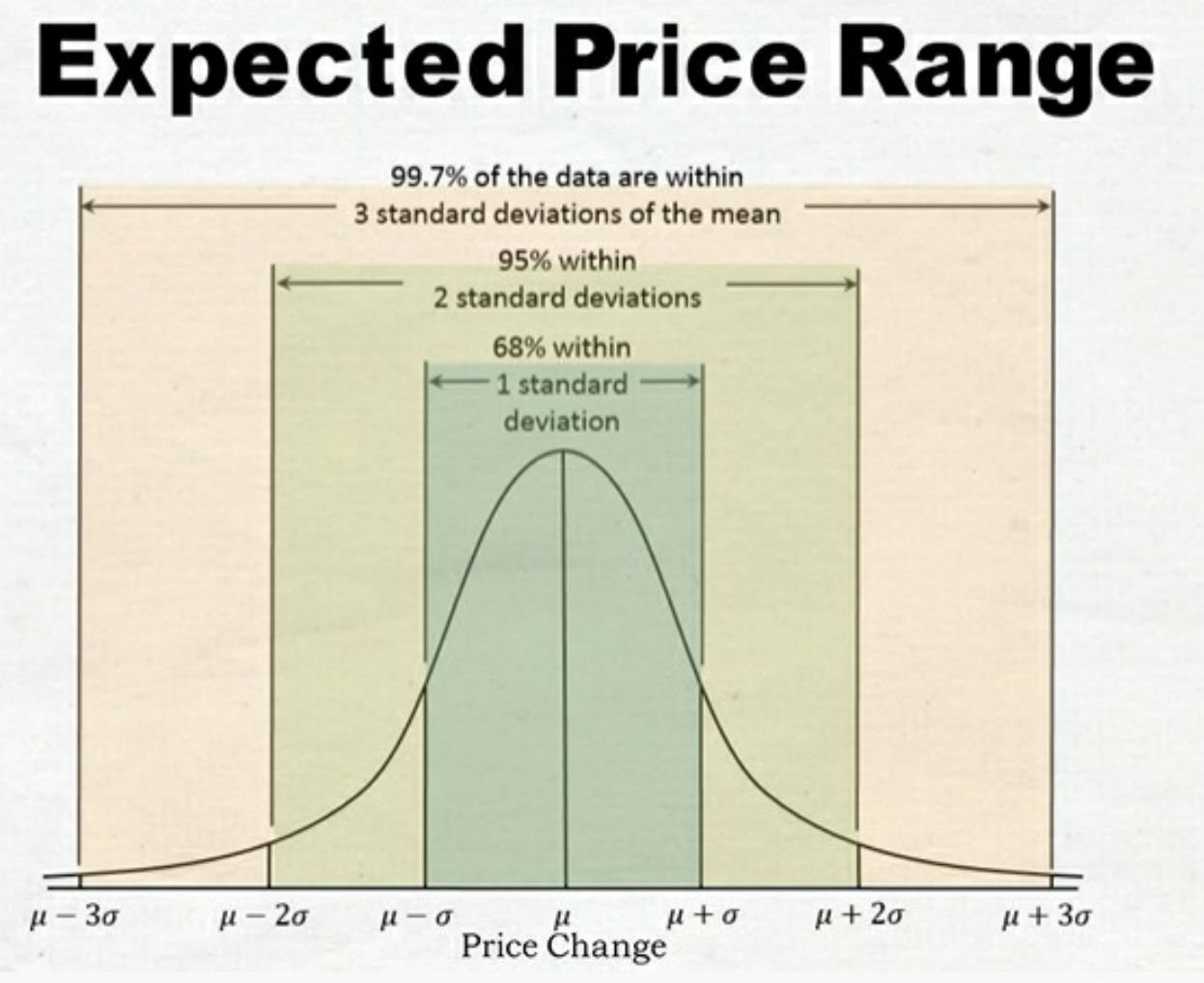
Chapter 36 Why Implied Volatility is Important

Well, first of all it's one of the main factors affecting an options price. This alone is one reason why you should pay attention to IV. Furthermore, implied volatility can give you insight into what kind of volatility the market is expecting. You can compare the expected volatility to your own analysis and potentially build a position around the difference in these two. An options trader should always look at implied volatility as well as the underlying trading price, expiration date and strike price before putting on a position. It's also possible to use implied volatility to calculate the expected price range of an underlying asset until the expiration date. To understand this let's first take a look at a normal distribution diagram.



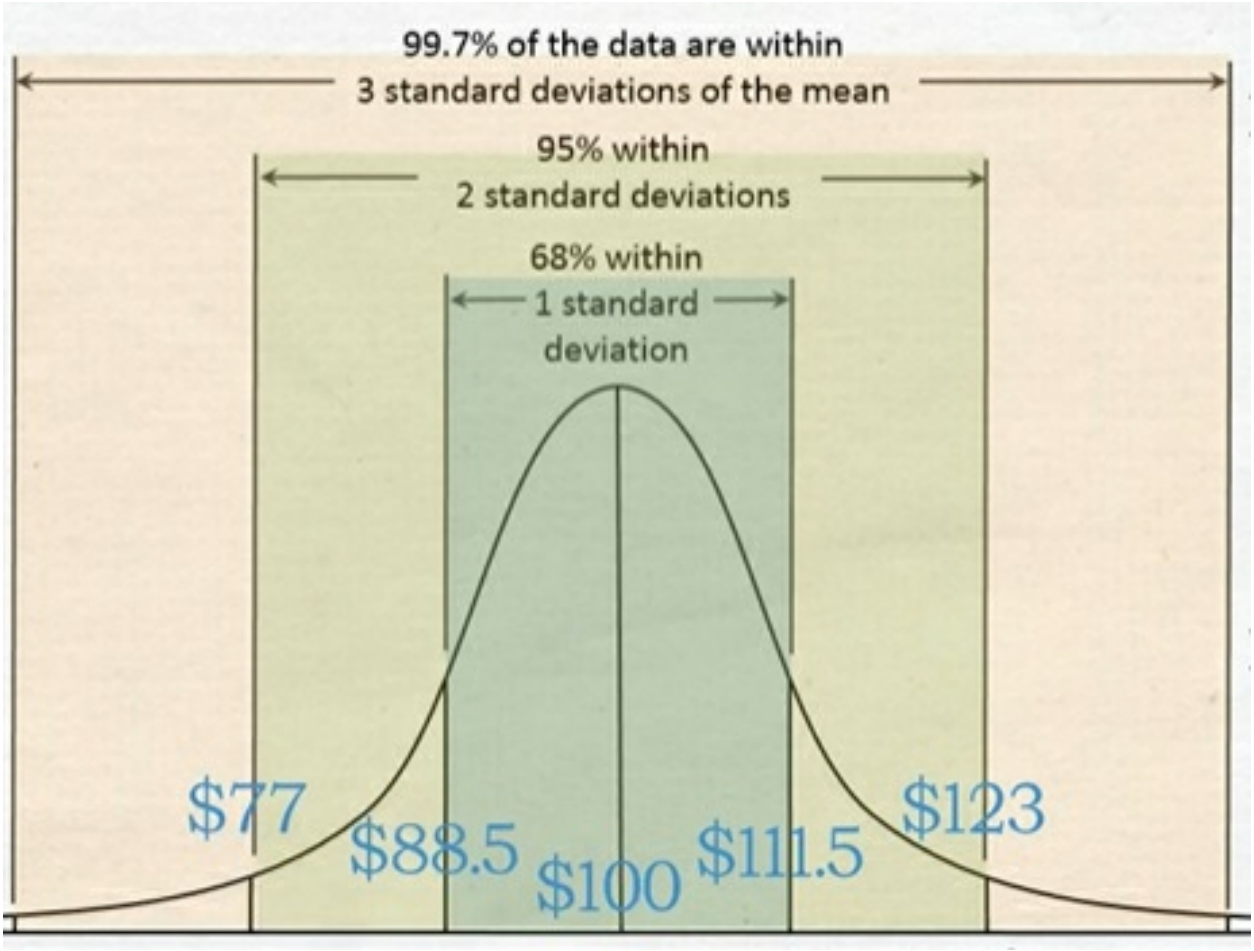
Depending on which model you use, you might assume that stock price changes are distributed like this. That would mean that 68% of the time price only changed slightly and the bigger a price move is, the less likely it becomes. The one standard deviation move for less happens about 68% of the time. The two standard deviation move where anything less happens about 95% of the time and so on. This isn't necessarily a very realistic distribution for prices because bigger moves happen far more often than they should according to a normal distribution. Furthermore, prices can move more to the

up side than they can to the downside. Nevertheless, a normal distribution is commonly used and it helps to understand what the expected move of an asset is. If you use the normal distribution you can calculate the expected move of an asset through this formula. One standard deviation equals, plus or minus implied volatility, times the underlying price, times the square root of the time to expiration divided by 365. Two standard deviations can be calculated by multiplying the one standard deviation move by two and so on.

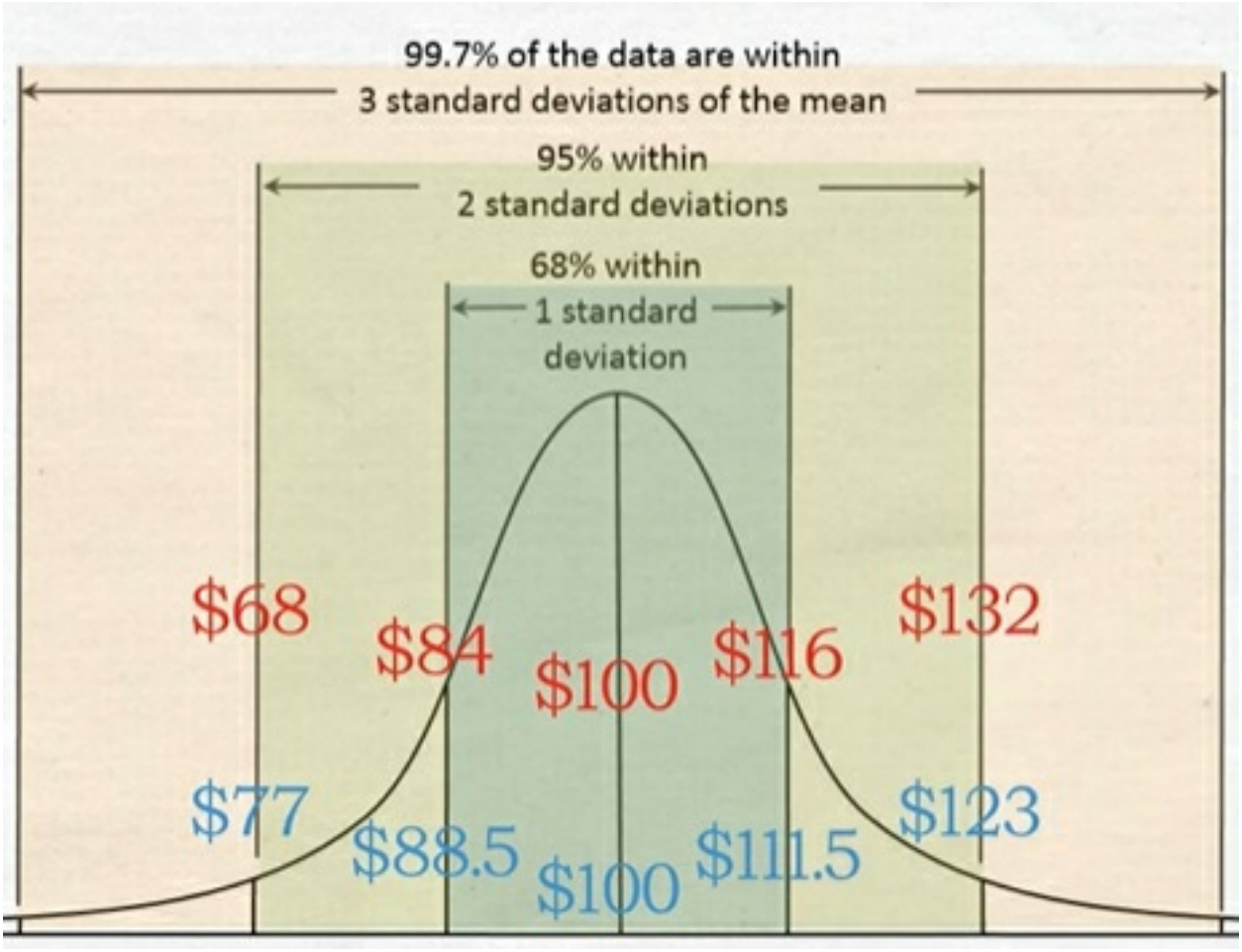


Implied volatility is normally quoted on an annualized basis. That's why we divide the time to expiration by 365 to get the expected range until the expiration date. Let's look at an example to clarify all this. Currency XYZ is trading at $100. We will first look at an option with 30 days left till expiration and an implied volatility of 40%. So the one standard deviation range over the next 30 days is plus minus 0.4, times 100, times the square root of 30, divided by 365. This is about plus minus 11.5 which means the

one standard deviation range over the next 30 days is 88.5 dollars till 111.5 dollars. This means that the markets expect XYZ's price to stay between about 88 and 112 dollars over the next 30 days with about 68% probability.



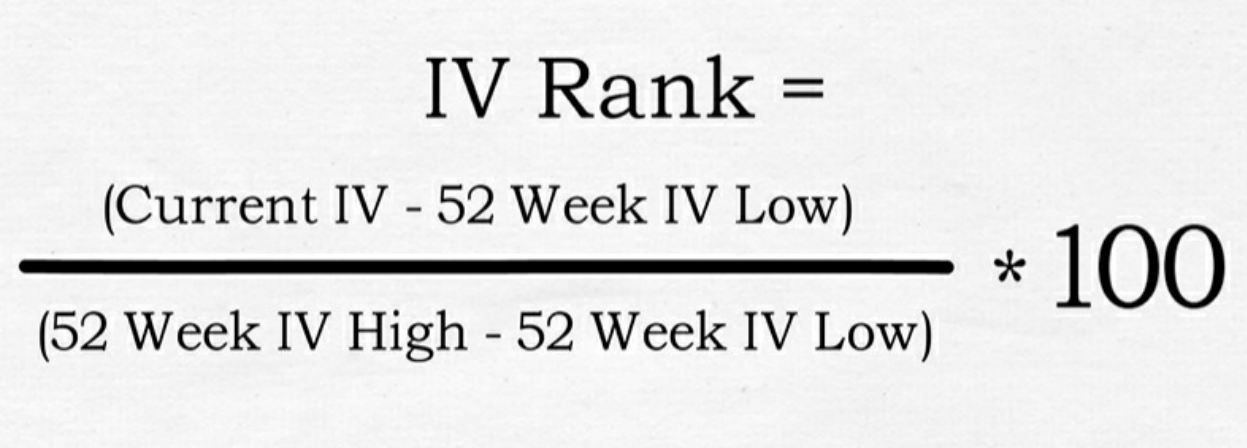
The two standard deviation move would be up to 123 dollars were down to $77. Now let's take a look at the same asset with the same implied volatility but 60 days instead of 30 days to expiration. The one standard deviation range would now be about 84 dollars to $116. The two standard deviation range would be 68 to $132. This makes sense because XYZ can obviously move much more in 60 days than it can in 30 days.



Note that all of this assumes that the distribution of prices is normal. This is not necessarily a very realistic assumption. Therefore in practice other distributions such as the log normal distribution or other ones are used much more commonly. Nevertheless, this simplified explanation of the expected move should give you a good idea of what the expected move is and how you can use it for your trading. Luckily, you will never really have to calculate the expected move yourself as most good broker platforms will calculate it for you.

Chapter 37 What is Implied Volatility Rank

By now you have hopefully realized that implied volatility is an important factor to look at when trading options. When implied volatility is high options are priced higher and when implied volatility is low options are priced lower. But how do you know if implied volatility is high or low? For instance, if an assert XYZ has an option with an implied volatility of 40% and asset ABC has an option with an implied volatility level of 30%, what does that mean? Well, just because the absolute implied volatility value of XYZ is higher than of ABC, we can't just assume that it's implied volatility is higher relative to itself. Let me give you a more specific example to clarify this. Let's say XYZ is usually a very volatile asset and has an average implied volatility of 70%. But now the IV dropped down to 40%, whereas ABC tends to have an IV level of around 20% most of the time. But now it's implied volatility has gone up to 30% and this means that ABC's implied volatility is relatively high and XYZ is implied volatility, is relatively low even though XYZ's absolute volatility is greater than ABC's. I hope that this explains that it's very hard to compare the implied volatilities of different assets, because different assets can have very different trading characteristics. To solve this problem, we can use implied volatility rank. IV rank looks at the past year of implied volatility data of an assets and then tells you how the current level of IV is relative to the past 365 days. IV rank is always a value between 0 and 100. 100 being the highest and 0 the lowest level of applied volatility over the past year. Here is a brief example. Asset ABC has an IV rank of 20. This means that it's implied volatility is relatively low because it has been much higher throughout the past year. Therefore you can assume that ABC's options are relatively cheap compared to past times. If on the other hand IV rank would be at 100, you know that ABC's implied volatility has never been higher over the past year and therefore this could be a good time to sell options because they are very expensive. In summary, implied volatility rank brings some context to implied volatility. Here is the formula that is most commonly used to calculate IV rank. The current IV level minus the 52-week IV low, divided by the 52-week IV high, minus the 52-week IV low and all of this is multiplied by 100 to get the IV rank.

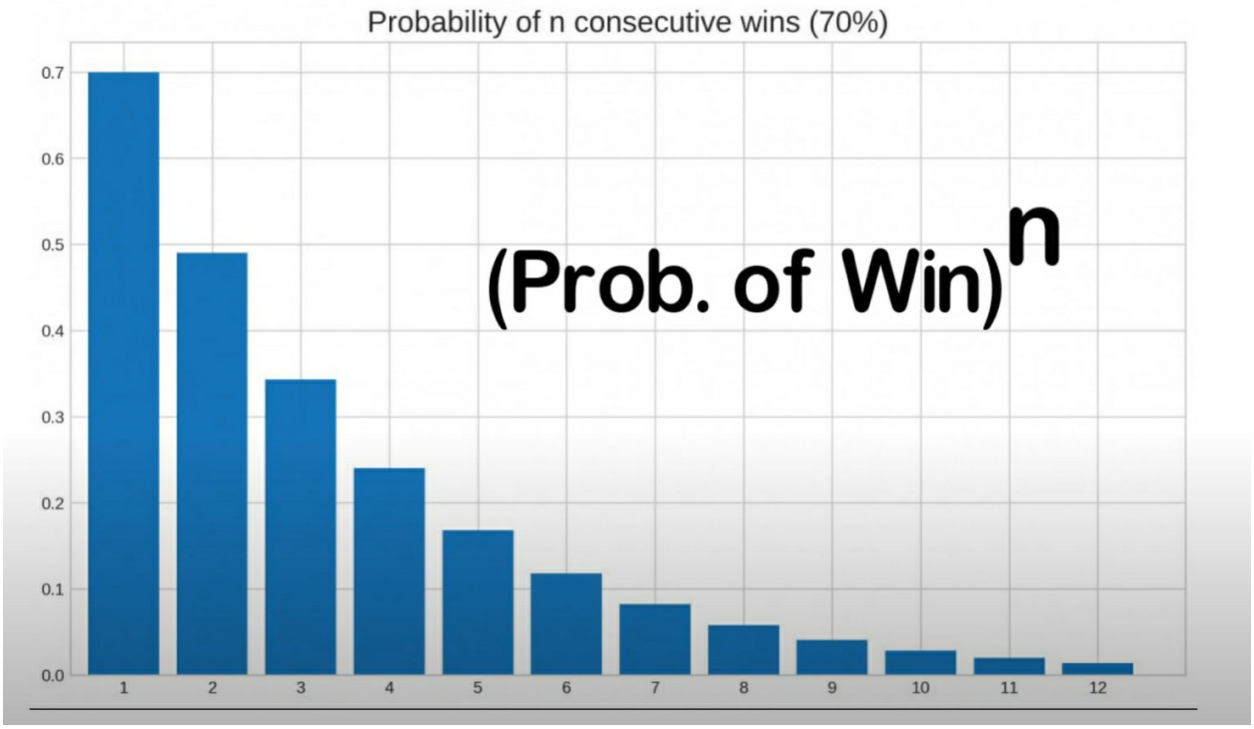


Note that some brokers often filter out very extreme implied volatility values from the past 52 weeks so that IV rank isn't skewed or distorted by these values. Don't worry you won't have to calculate this yourself because once again most good brokers will do this for you. Certain platforms even allows you to scan and filter assets by IV rank. This is one of the easiest ways to find assets with very low or very high implied volatility values. I hope this helps you understand implied volatility and how implied volatility rank works.

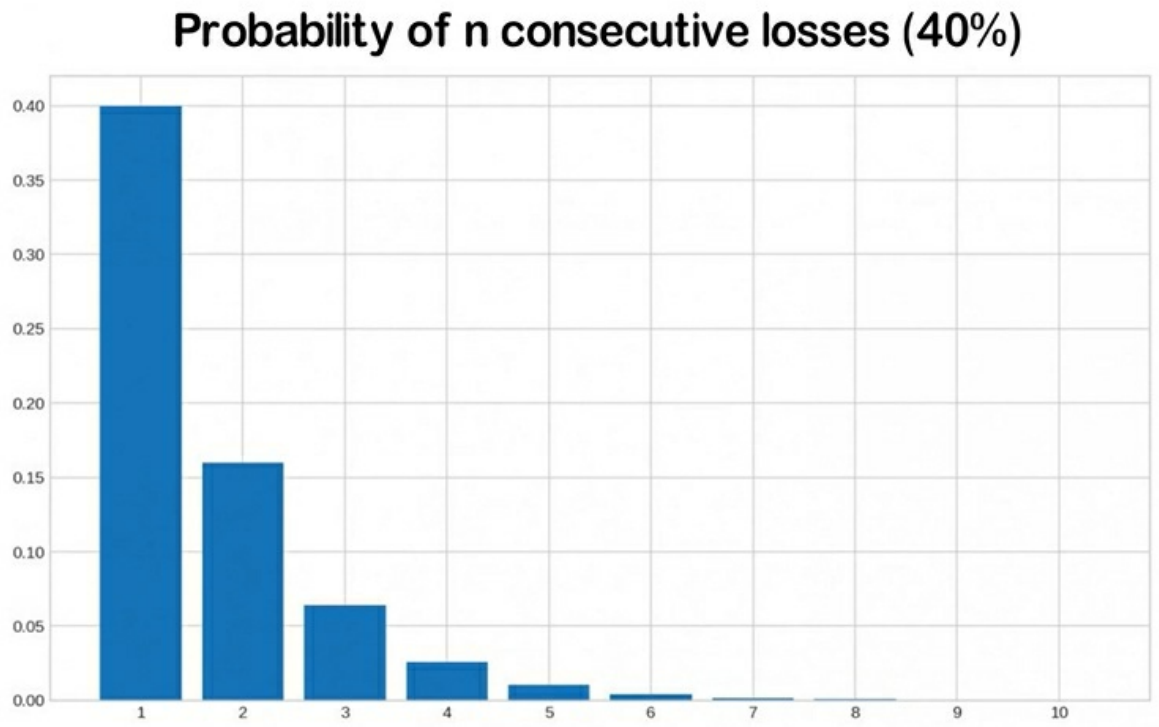
Chapter 38 Trading Psychology: Gambler's Fallacy

While most people like to think that they are rational, most humans aren't very rational. Especially when money is on the line and time is scarce human decision making can be very flawed. Trading is one of the fields where erroneous and irrational behaviour patterns are especially common. In this chapter we're going to look at the most common cognitive biases and irrational decision making patterns and how to avoid them. Being aware of these thinking flaws has two main advantages. Firstly, it helps you avoid them in your own trading and secondly it can help you identify and explain seemingly irrational market behaviors caused by these biases. Most of these so-called cognitive biases were discovered and introduced by the Nobel winning Daniel Kahneman and Amos Tversky. The first cognitive bias that I want to talk about is the gambler's fallacy. The gambler's fallacy is incorrectly over or understating the likelihood of an event based on a series of past events. This can be illustrated with a simple example of a coin flip. The probability that a coin will land on heads is 50%. No matter how often you flip a coin this probability does not change. So even if your coin just landed on heads 10 times in a row, this does not affect the probability of the next coin flip. Like the name implies, the gambler's fallacy is especially common in gambling. But this pattern of thinking is quite common in trading as well. Let me give you some examples. Have you ever opened a long position because a stock had many consecutive down days or vice versa? If so, you have fallen prey to the gambler's fallacy. Another example would be the reaction to a losing or winning streak. If you ever felt that after many consecutive wins the chances of losing increased and you decreased your position size, you have been guilty of the gambler's fallacy. The odds of winning on a trade, don't magically change just because you had multiple losses or wins before this trade. Speaking of winning streaks if we assume that you found a trading strategy that guarantees you a 70% chance of winning on every single trade, what do you think the odds of winning 10 times in a row are? Well, the answer is under 3%. In fact, even the probability that you will have two consecutive wins with this strategy is under 50%. This means it is less likely that you will have two consecutive winners than that you won't. And remember, this is with a strategy that guarantees you 70% chance of success on each trade. Most strategies won't have nearly as good

odds. To calculate the probability of “n” consecutive wins you simply have to take the estimated odds of your trading strategy to the power of “n”.



Note that this assumes that the trades are independent from each other and the probability of winning is constant. If we look at the odds of losing streaks we get a similar picture. Here's a diagram that shows the probabilities of multiple consecutive losses with a trading strategy that has a 40% chance of losing on any single trade.



As you can see with a 40 chance of losing it is extremely unlikely that you will have more than a handful of losses in a row. So what can we learn from this? Firstly no matter how good your strategy is, losses do happen. You can't win all your trades. Therefore you have to implement solid risk management practices and keep the size of your losses under control.

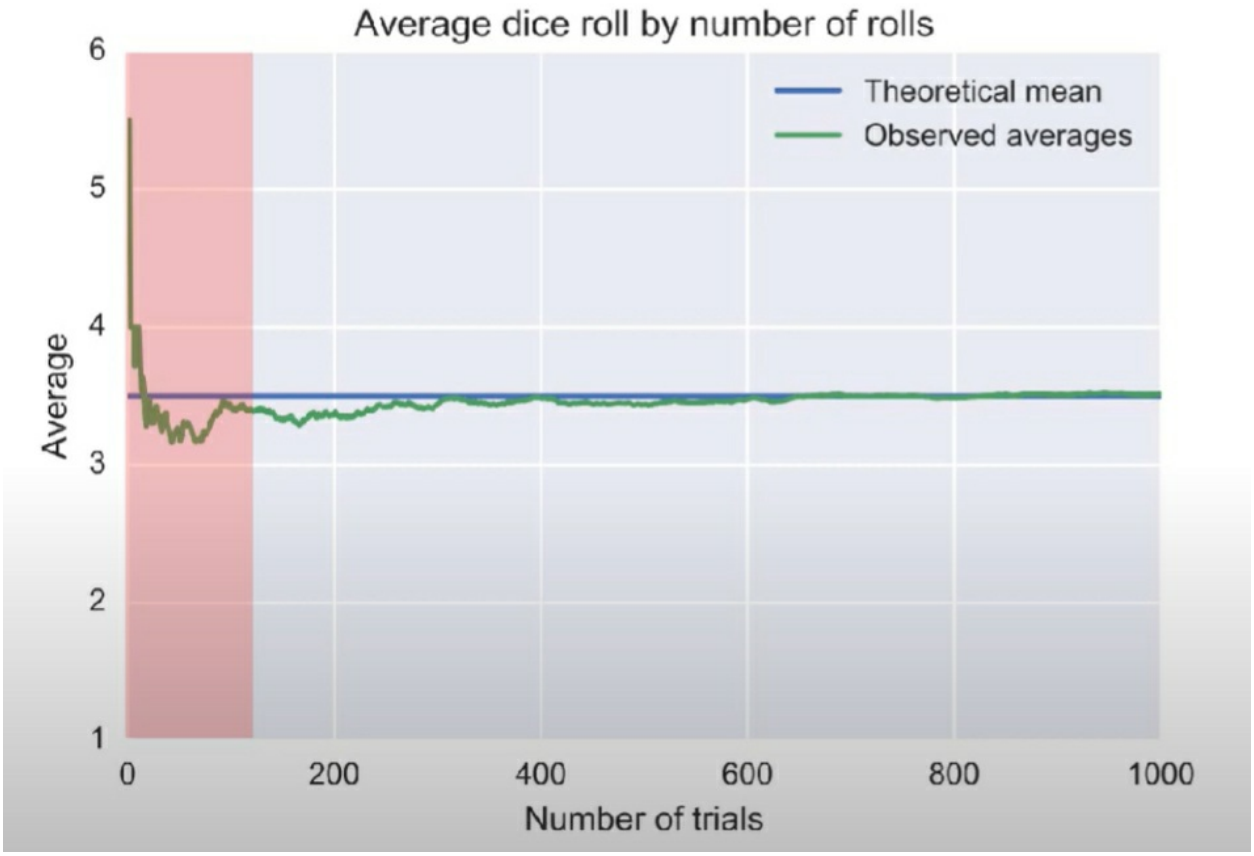
The odds of having many losses or wins in a row is quite low. So if you often have more than 10 major consecutive losses, you should seriously start doubting the quality of your trading strategy. But always remember, even though the probability of winning 10 trades in a row is very low, the probability of winning on any single trade is not lower just because you won on the last 10 trades.

Chapter 39 Trading Psychology: Confirmation Bias

The confirmation bias is the tendency to seek out information that confirms your pre-existing beliefs. This is a bias that without a doubt, the vast majority of traders have been guilty of. After opening a trade it is only natural to continually seek out information that confirms your trading idea. You might look at dozens of indicators or social media posts and only focus on those that confirm your beliefs. Finding something that agrees with you is a good feeling and certainly can boost your confidence in a position. The problem is that by doing this you often ignore signs that your trade wasn't the best idea and something might be wrong. Instead, you convince yourself more and more that everything is fine. By searching Twitter for a ticker symbol you're almost guaranteed to find at least a few people that have the same market assumption as you. But this doesn't mean anything. One way to avoid confirmation bias in trading is by having a clear set of indicators and rules to follow for your trades. If you have such a clear set of rules and indicators, there is no need for you to go out and look for any other confirming signs. Furthermore, it is best to avoid social media as a trade decision making guide.

Chapter 40 Trading Psychology: The law of Small Numbers

You might have heard about the law of large numbers that states that the average of a growing sample size converges to the actual mean of the total population. This is a very powerful rule in probability theory that allows you to estimate a population's parameters with large enough samples. But like the name implies, this only works for big sample sizes. This is where the fallacy of the law of small numbers comes into play. Most people intuitively use the law of large numbers incorrectly, namely with two small sample sizes. Let me give you an example. Have you ever tried a trading strategy for a handful of trades and then concluded that it doesn't work? If so, you have been guilty of using the law of small numbers. A few traits is not a big enough sample size to give you any significant information about the quality of a trading strategy.



How you can avoid the law of small numbers? Well, you have to efficiently test the effectiveness of a trading system. The goal is to use this trading system for at least 20 trades. It might seem scary to use a new trading system

for over 20 trades when you have no idea how good or bad it might perform. Therefore you should trim down your risk to a level so that you can easily afford to lose on all these 20 trades. Your goal with these trades is not to make money, but to test out the given trading strategy. When making these 20 trades try to be as mechanical as possible. Create clear rules for every market scenario imaginable and follow these rules on every trade. If you don't have a clear set of rules to follow, you can't reliably test your strategy since there is no strategy to test. Furthermore make sure to keep a detailed and thorough trade journal. After every trade, track entry prices, exit prices, profit potential, money at risk, time in a trade and more. After you've followed all these steps for at least 20 trades, you're ready to evaluate the strategy. Ideally you should now have a rich collection of data on this strategy to evaluate it and make an informed decision on how effective this trading system is. I know that this might seem like a lot of work just to test the trading system but without having a big enough sample size, you can't really evaluate anything. Making a decision based on one or two occurrences, is like saying roulette has a 100% win rate because you won one round.

Chapter 41 Trading Psychology: The Survivorship Bias

The next cognitive bias that we're going to look at is the survivorship bias. Wikipedia defines survivorship bias as “The logical error of concentrating on the people or things that made it past some selection process and overlooking those that did not, typically because of their lack of visibility.”

Let's once again look at a couple of examples to better understand what this means. If you look around it is easy to arrive at the conclusion that most ETF-s Mutual funds and even individual stocks go up over time. But in reality, this is a wrong conclusion. That's because the universe of funds and stocks that you look at, is already skewed in one direction. One reason why stock did not go up but instead fell is that it went bankrupt. And a bad performing fund usually gets closed after a few years. In other words only those funds survive that performed well enough. So when you say that most stocks or funds go up over time, you aren't considering all those that didn't survive. Therefore the results obtained by only looking at survivors can be vastly flawed. To give you some data a Vanguard group study recently found that an investor in a large cap growth or value fund in 1997 stood just a 22% chance of finding a fund that would survive and outperform its benchmark through 2011. The problem of only considering a universe of investments that survived a certain selection process is especially common when back-testing and analyzing trading strategies on historical data. But also when analyzing success stories outside of trading, survivorship bias can be a big problem. The results of looking at shared trades of highly successful people, doesn't actually yield very significant results. Typically, many unsuccessful people also share these traits but they weren't considered in such a study which can dramatically skew the results. Often successful people succeed in spite of certain traits, not because of them. The phrase that history is written by winners very much also applies in business and financial markets. In general, when looking at and analysing investments make sure to think about that what you can't see. Is there a seemingly invisible filter that you are missing? If so, your results can be vastly skewed in an unwanted direction.

Chapter 42 Trading Psychology: Correlation

Correlation does not imply causation but sadly it is often treated as if it does. There are different types of this fallacies so let me cover three of the most prominent causation fallacies. The first is reverse causation. An easy example of this is the correlation between rainy days and the usage of umbrellas. When it rains people tend to use umbrellas much more. Does that mean that using umbrellas causes it to rain? Of course not. It's the other way around. This might seem like an obvious mistake, but often things aren't as clear. If for instance asset A and asset B are heavily correlated, does that mean that an opt move in A's price causes a reaction in B's price or the other way around? Another causation bias is neglecting the fact that the third variable might be the cause of two correlated variables. For example two oil stocks might be highly correlated but this doesn't mean that a move in one of the stocks causes a move in the other stock. Instead, a third variable namely the price of oil might be the cause for the moves in both of these stocks. Last but not least, two variables can also be correlated without having any causal link. In fact, if you have a big enough set of data, you're almost guaranteed to find some variables that are correlated purely by chance. One example of such a coincidental correlation is the correlation between per capita consumption of chicken and US crude oil imports. These two variables have a historic correlation of almost 90% over about 10 years. Nevertheless, I wouldn't use chicken consumption data to try to predict US crude oil imports. There are countless similar examples of seemingly nonsensical correlations. So going forward never assume that correlation means causality. Proving correlation is very straightforward, but proving causality is a totally different story.

Chapter 43 Trading Psychology: Hindsight Bias

Hindsight bias is the tendency of overstating the odds of an event that has already happened. Here is a great quote from Nobel prize winning Daniel Kahneman about hindsight bias. “A stupid decision that works out well becomes a brilliant decision in hindsight.” Hindsight bias is especially common amongst traders. Way too many traders evaluate the quality of their trades based on their outcome. This is a very flawed way of evaluating your trades. A trade that has a 70% chance of making 200 dollars and a 30% chance of losing 100 dollars is without a doubt a great trade. No matter its outcome, even this trade won't work out three out of ten times. But that doesn't make it a bad trade. Sadly this is how many traders evaluate their trades. Hindsight bias is also the reason why technical analysis seems so attractive. Finding chart patterns on historical charts is very easy, but without the benefit of hindsight things aren't nearly as easy. If you ever felt that the past price move seemed so obvious, you have fallen prey to the hindsight bias buyers. To avoid hindsight bias, you need some way of evaluating your trades not based on their outcome. Instead you should focus on the quality of your decisions along the way. Did you have a clear trade plan and strategy? If so did you follow it? If not, why not and what could you do better next time? In general, it is best to have a consistent way of evaluating your trades that is not affected by the outcome of your trades.

Chapter 44 Trading Psychology: Recency & Attribution Bias

Recency bias is the illogical way of putting more weight and importance to recent events, compared to historical ones. This can easily be observed by looking at the cyclical nature of markets. The longer a bull market is, the more and more people forget that prices don't only go up. Thus investors pay less and less attention to their risk, even though it should be the other way around, since the further prices rise the more they can fall. The same is the case directly after market crashes. This is when people typically over manage their risk because they overestimate the odds of future drops. This can be a great time to sell overpriced insurance products such as options and volatility.

A different bias that can be observed in the trading news business is the attribution bias. The attribution bias is the bias of constantly trying to assign some reason to an event, even if your reason has nothing to do with reality. Financial news companies are in the business of satisfying this bias. They seem to have an explanation for every single price move, even if their explanations sometimes are contradictory. Sometimes you can't break down a price move into a simple cause and effect relationship. But this doesn't stop us from trying. The problem is that humans are very good at finding an explanation for almost anything, even if the explanation doesn't make sense. Basic traits on these explanations can do more harm than good. So make sure to be careful when looking at the reasons that financial news organizations assign to certain price moves. The best explanation for an up move, will always be that they are simply more buyers than sellers.

Chapter 45 Trading Psychology: Sung Cost Fallacy

If you ever held onto a position far longer than you should, you have been guilty of this fallacy. The sunk cost fallacy is the tendency to refuse to stop an action because you've already sacrificed a good amount of money and or time into it. Sometimes it's best to just cut your loss than to further waste money and time on a project or trade. Some costs should not be a reason for you to stay in a trade. If you wouldn't open your trade at its current price level, you should not stay in it. Regardless of how much you already have lost. One way of combating the sunk cost fallacy is by having a clear trade plan with clearly defined exit points before you enter a trade. We have now covered a wide variety of different cognitive biases that can dramatically impact your trading and decision making in general. Let me now cover briefly look at how you can avoid these biases. First and foremost, it is already a good step in the right direction to be aware of that these biases exist. But sadly, simply being aware isn't enough to completely avoid them. In fact it is almost impossible to fully eliminate these biases from your life, since they are so deep ingrained in your human psychology. That said you can definitely do things that can reduce the frequency of them and thereby improve the quality of your decisions. One thing that can dramatically increase the likelihood of using these cognitive biases, is trying to make a decision under time pressure. So avoiding time pressure is another step in the right direction. One way of avoiding time pressure in trading, is by preparing beforehand. Instead of trying to improvise and rely on your intuition always have a clear trade plan before you open a trade. The trade plan should have all the information you need to mechanically carry out your entire trade. Besides a trade plan, a good trade journal is another way for you to improve upon your decision making and trading. Otherwise try to actively monitor yourself for these cognitive biases. Especially in situations where the likelihood of a bias is high, step back and rethink the entire situation from another perspective. Furthermore, avoid making important decisions when you're in a bad mood or not fully focused due to a lack of sleep. For instance if you are interested in learning more about this topic I highly recommend checking out Daniel Kahneman's book called “Thinking fast and slow”.

Chapter 46 Trading Psychology: Winners & Losers

In this chapter I will explain how you can develop a winning attitude in trading. But first of all, why psychology and trading even important. Well, trading is a very unique activity. It's unlike every other activity that you can imagine. In some cases even contradict some beliefs that we have acquired throughout our lives. Let me give an example of this. Most people think that the more work you put into something the better results you will get. For instance most jobs are paid on a per hour basis but this isn't necessarily the case for trading. Just because you spend countless hours analyzing the fundamentals, the technicals or anything else of an asset doesn't mean that you will make money. You may very well even lose money and a trade that you spend countless hours preparing. Trading is a very emotionally demanding activity. Seeing your hard-earned money vanish in front of your eyes isn't easy. But also huge gains do affect your emotions. Trading confronts us with constant uncertainty. May very well lose money on a day but you may also very well make money. It's not uncommon to see people lose weeks or even months of gains on one bad trade. Nevertheless, it is important to try to avoid emotional trading. Letting emotions influence your trading decisions can dramatically decrease your trading performance. It can be very hard to control your emotions when hard-earned money is on the line. There are five fundamental truths that can help traders to develop a winning mindset. First of all, anything can happen. In essence, the markets aren't anything else than millions of different people expressing their thoughts about different assets. People that think in assets prices low will likely buy, those that think in assets prices high will sell and others will wait for a better opportunity. But every single trader of these millions of people can impact the price. Therefore theoretically anything is possible. But even though everything is possible not everything is likely. The probability that an assets price will rise by hundreds of percent is relatively slim. However the probability is not zero. It is possible. This brings us to the second fundamental truth. You don't need to know what is going to happen next in order to make money. You don't only don't need to know what is going to happen next. You can't know what is going to happen next. We just learned that the markets aren't anything else then millions of people expressing their beliefs. If you know what's going to happen next, you would have to be

familiar with the beliefs of all of these millions of people interacting with the markets. It's safe to say that this is impossible but that doesn't matter you can still make money in the markets. If you have the trading system with the true edge it really does not matter what's going to happen next? Well, the outcome of next trade is irrelevant. For example a casino has a true edge. The odds are on their side. Let's take roulette as an example. The casino has a higher probability of making than losing money on a game of roulette. However they do not know what's going to happen on the next roulette spin, nor do they care. They may very well lose money on the next spin of roulette. But that doesn't matter to them because they know that they will win in the long run. The same goes for your trading. As long as you have a trading system with the real edge all you have to do is stick to that trading system. The outcome of your next one two or even more trades does not matter. As long as you stick to your plan, the numbers will work themselves out in the long run. The next fundamental truth is that there's a random distribution between wins and losses for any given set of variables that define an edge. This goes hand-in-hand with the previous truth. Just because the odds are in your favour does not mean that you will be right. Let's look at our casino example once again. The odds of winning a game of roulette are strongly in the favor of the casino. However that does not mean that they will win guaranteed. They will still lose money on some games. If you really believe in a random distribution between wins and losses, could you really ever feel betrayed by the market? If you flip the coin and guess right, you wouldn't necessarily expect to be right on the next flip simply because you were right on the last. Nor would you expect to be wrong on the next flip if you were wrong on the last flip. Let's move on to the next fundamental truth. An edge is nothing more than an indication of a higher probability of one thing happening over another. Hopefully this is relatively simple by now. Once again I'd used the casino example to explain this. In a game of roulette, the casino has a higher probability of making than losing money. So that is their edge. The final fundamental truth is that every moment in the market is unique. If this wouldn't be the case, it would mean that every single person and entity that interacted with the market during a previous moment would have to do the exact same thing again. They would all have to enter and exit their positions just like last time. This is more or less impossible and therefore every moment in the market is unique. If a moment isn't unique you would have to know every variable which once again isn't possible. So what are the

takeaways of these five fundamental truths? Well, first of all you do need a concrete trading system with concrete rules. Otherwise, you wouldn't have an edge and then trading would be pointless. Remember, random trading will lead to random results. Besides a trading system, you also need a trading plan. You should always create a trading plan before every trade. It's very important that you create your trading plan before you open a trade because that's the only moment where you still are able to think 100% rationally. After you enter a trade your hard earned money is at risk and then your emotions will influence your decision making. Some key components of your trading plan should be your max risk, your max reward, your risk to reward ratio, your exit point, your entry point, your adjustment point, your position size and ideally even more. If you truly believe in the five fundamental truths, you will automatically create a trading plan before every trade. For instance if you actually believed that you don't know what's going to happen next and anything is possible, you would always define your risk and cut your loss. If you believed in your edge and all the truth why would you do it from your trading plan. Why would you revenge trade or double up to make back the losses from a previous trade. Why would you ever feel emotional pain if you believed in your edge. Does a casino feel emotional pain just because it lost on a single game of roulette? No, and neither should you. The more specific your trading plan is the better. If you have trouble sticking to your trading plan write it down. In theory, your trading plan should be so concrete that you would be able to give it to someone else who then could execute the entire plan without having to ask you. The more specific a trading plan is, the less you will have to think about what you're going to do and thus you will trade more mechanically. Another tip for trading more mechanically is using trade alerts. If you know that they're going to exit or adjust a position if a price reaches a certain point, you can set an alert at that point. As soon as that price will be reached, you will get notified and can adjust your position without having to think about it. Alternatively, you could use automated orders like stop losses or take profit orders. But probably one of the most important takeaways is that you should trade small. You should never risk more than a few percent of your total capital on one trade. If you truly accept the risk before entering a trade and keep your position sizing small, you will never ever have trouble sleeping at night. Remember that you don't and can't know it's going to happen next and therefore it's not unlikely that your next trade will be a loser. If you risk all of your capsule at once and the next trade

will be a loser, you will lose all of your capital at once. That's a disaster that you should never risk. This is also why casinos said betting limits. They know that they can very well lose on a single game of roulette. If someone wants to bet millions of dollars on a single game of roulette, the casino will likely decline. Because it knows that the odds aren't heavily in its favour. Their edge only really works in the long run when the number of occurrences is high enough. You should think the same way with your trading. So never risk too much of your capital at once. If you're currently familiar with the seemingly profitable trading system but somehow can't manage to be consistently profitable with it, it might be due to your mindset. So instead of trying to learn tons of new trading strategies, you could try to focus more on your psychology.

Chapter 47 Step by step checklist for a Trading Plan

One of the worst mistakes beginning traders make is to not pay enough attention to their trade entries. Neglecting the importance of a good entry and exit can make a huge difference to your bottom line. In this chapter you will learn all the do's and don’ts of opening and closing trades. Before we get into the nitty-gritty of actually setting up the best possible trade order, let me first talk about how to set your trades up for success. One of the biggest mistakes that you can make is to not have a clear trading plan. Without a plan you're basically trading blind. To help you always have a trading plan from now on I'm going to present you a step by step checklist that walks you through every aspect to consider before sending any trade order. If you go through all these steps you should never again be in a trade that you don't know what to do with. Let's now go through this trading plan template. First of all I recommend taking a look at upcoming events. Even though this doesn't directly affect your trade looking at future events before opening a trade can save you from unwelcome surprises. Are there any upcoming dividend payments earnings or other upcoming events that might clash with your trade plan? Around these events stocks often behave differently and they normally would. So either be aware of this or avoid trading through these events. Next, define your risk. Never open the trade without knowing your max loss. Way too many traders don't do this even though this is a must for you to be able to manage the risk. Besides defining your risk you should also define your reward. Have a clear profit target that tells you when to take profits. Without a clear profit target it's easy to tell yourself to wait for just a little more. Doing this will lead to winning trades turning into losing ones. After defining your max risk and Max reward is very easy to calculate your risk to reward ratio. So make sure to do exactly that. Actually calculating and seeing your risk reward ratio will give you more insight into the payoff of your trade. A good rule of thumb is that your risk to reward ratio is better than 1 to 2, but note that you should also take the probability of profit into account. It's totally ok that your risk is greater than your reward as long as your probability of profit is high enough. Furthermore, you should also define the time frame of your trade. Is it a day trade, swing trade or long term investment. You don't need to know the exact time that you're going to be in the trade but you should have an estimate of the trades time frame. Inside of

your trade plan you should also have a concrete entry plan. This plan should entail your entry price, position size and how you want to open your trade. Do you want to open the entire position at once or slowly average into it? Lost as important is your exit plan. This should describe how you're going to close your position. This could include possible trade adjustments, your trade exit price and exit trigger. The most obvious exit trigger would be a certain price level. But it certainly isn't limited to that. You could for instance also use a timeframe, probability of profit, certain indicator values or the P&L of your position as an exit trigger. Moreover, your exit plan should include how you're going to close the position. Last but not least, a trade plan could also include other notes such as the motivation behind the trade, your directional assumption, a trade description or something else. Hopefully this template gives you an idea about what a good trading plan could look like. It's very important to create such a trading plan before you open your trade. This allows you to stay rational and clear-headed. As soon as you open your trade, you lose the ability to evaluate the position objectively. Furthermore it's a great idea to actually write down your trading plan. Especially for beginning traders this is a good exercise. With time you will be able to do this in your head, but like everything this requires practice. So even though writing down your plan takes time it will force you to really think about your trade. This is also a great counter against impulsive trades or Gamble's. If you ever again find yourself in the situation that you have no clue what to do with your trade, just take a peek at your trading plan and you will see the answer to this question. After you close a trade you should always ask yourself; did you stick to your trading plan? If you didn't, why not and what could you do better next time? If you did, was it a good plan or how could you improve the plan next time? Asking and answering these questions will allow you to continually improve your trading plans and thereby your trades. A great place to answer these questions is in your trading journal. Having a good trading journal is another great way to evaluate your trades without falling prey to cognitive biases and subjectivity. If you currently do not have a trading journal I highly recommend starting one as soon as possible.

Chapter 48 How to set up a Trade Order

Even though setting up an order might seem like an easy task, there are still are many things that you can do wrong. For example the biggest mistakes

that many traders make is using market orders. A market order gives you the next available price. This will get you filled very fast but more often than not the price will be bad. So what should you do instead? Well, instead of market orders, use limit orders. Limit orders allow you to set a fixed price at which you want to get filled out. Either you will get filled at this price or you won't get filled at all. As long as just don't set your price too aggressively and the security is liquid enough, you will get filled at your desired price anyway. But even if your order isn't filled it is often better to miss a trade and to accept a bad entry price, since a bad entry price would mean more risk and less profit potential. To choose a good limit price it is important to understand how the “Bid-Ask Sread” works. The bid price is the highest price a buyer is willing to buy the underlying security for and the ask price is the lowest price a seller is willing to sell it for. The bid-ask spread is the sprint between these two prices. To get filled as fast as possible, you need to move closer to the ask price when buying and closer to the bid price when selling. For most securities however these prices change all the time. Therefore you can often get filled at the mid-price. That's also why I recommend always setting your limit order price at the mid-price to begin with. If this doesn't get you filled, you can always readjust later on. Ordering at the mid-price can save you thousands of dollars over the long run. Last but not least I recommend setting your orders to expire at the end of the current trading session. But if you don't want this you can always choose a good to cancel order. This order type will stay active until it is either failed or you cancel it manually. This is especially useful to automatically take profits on a given trade. For instance, if you know your profit target you can just send out a good to the concert order as soon as you open your trade and let the order sit. The same can be done for the downside with a stop loss. An alternative to good to the cancel orders are good to date orders. The only difference between the two is that good to a date expire after a certain preset days whereas the good to cancel order has to be concert manually unless it's filled. Some brokers even offer bracket orders. These are also known as one cancels other orders. Such an order allows you to send out two orders one to take profits and want to cut losses and as soon as one is filled the other one is automatically cancelled. This is a great way to automate your trading plan. It's hard to make discretionary trading more mechanical than this. Last but at least here are some tips to get feel it faster First of all, make sure to trade liquid securities. If you aren't trading liquid securities fails will take much

longer and even worse, it will leave a lot of money on that due to a wide bid-ask spread. If you're trading options you could analyze option chains for options with high open interests and volume. Getting filled on these options is much easier than other ones. The next tip would be to scale into your trades. Instead of opening your entire position in one order break it down into multiple smaller orders. This can decrease field times dramatically. Note that you should only try this if your broker's commission structure doesn't charge you too much for each order. Otherwise, placing orders at route numbers can often help you since route numbers typically attract much more stop losses and limit orders than other prices. If none of these things help, you could always move your price closer to the bids or ask price. But only do this if the new price is still good enough. In summary, you should always have a clear trading plan and make sure you create this before your trade. If you don't know how to create a trading plan just use my template from the previous chapter. Furthermore, make sure to keep a trading journal so that you can track your progress and learn from your mistakes. Otherwise, don't use market orders but instead use limit orders. A good limit price to start with is the mid price. Last but not least focus on trading liquid securities with high-volume, otherwise you're just throwing money out of the window.

Conclusion

Thank you for purchasing this bundle book. If you enjoyed the book, please take some time to share your thoughts and post a review. It would be highly appreciated!