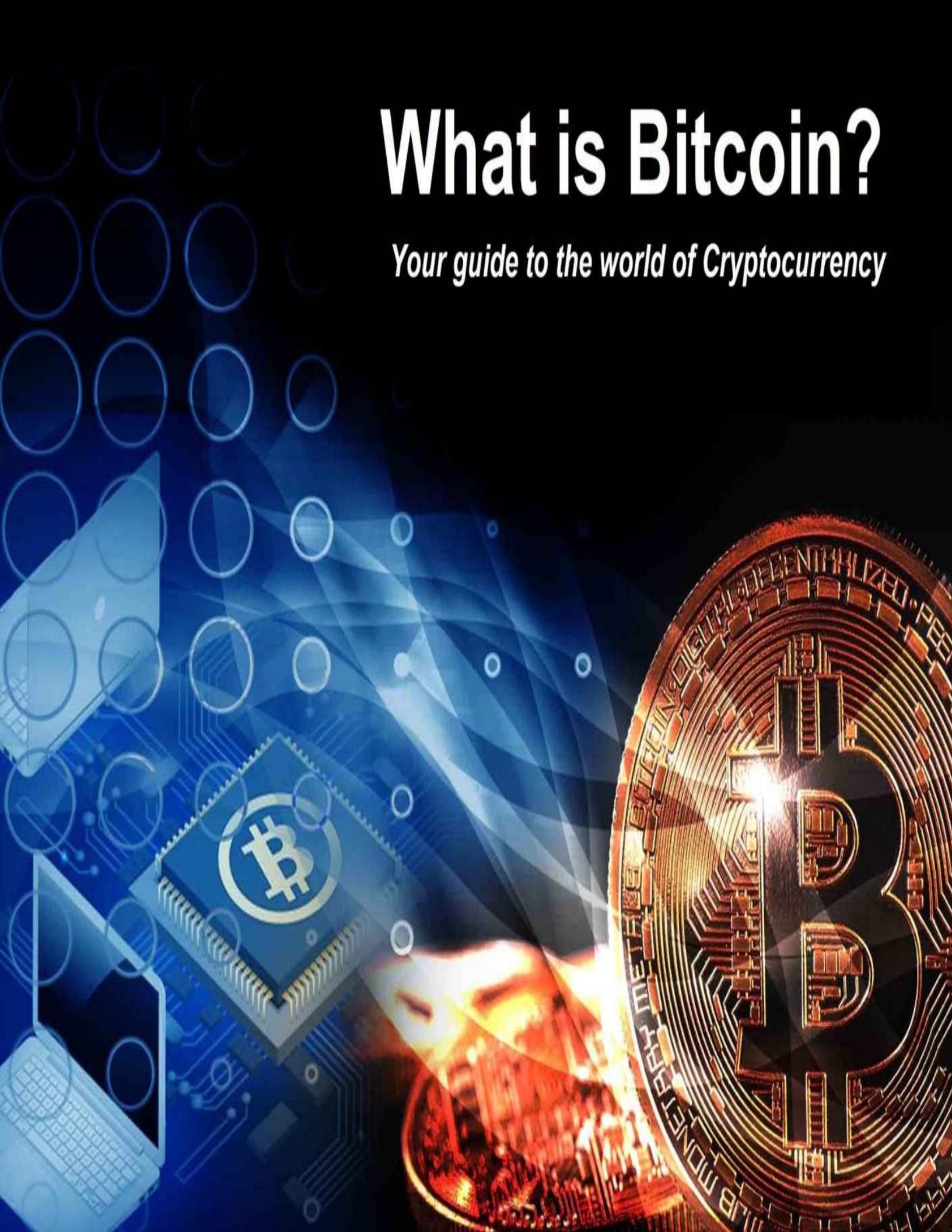
What is Bitcoin?

Your guide to the world of Cryptocurrency



Bitcoin, Blockchain, and Cryptocurrencies.

Dear reader:

In the lines that follow, please find our concise introduction to useful concepts in cryptocurrency, of which BitCoin is at this time the best-known example. The pamphlet is friendly to a non-technical reader.

Bitcoin is by now basically one cryptocurrency among others, but also, an influential and clever one, which introduced the notion of the blockchain. The blockchain is an accounting system within the currency.

It is this key invention that made other competing cryptocurrencies, possible.

In turn, there are some initiatives to abstract the blockchain away from the currency itself, and we will describe these as well, once it is made clear how the exemplary notion might itself -- with compromises -- be separated from its origins. The pamphlet is therefore organized as follows.

1. What is cryptocurrency
2. What is Bitcoin?
3. What is blockchain?
4. What can it be used for?
5. Who can use it?
6. How can I use it?

A note on usage: BitCoin and Bitcoin are the same thing.

The authors thank you for your time.

1. What is cryptocurrency

A cryptocurrency is an alternative form of commodity exchange which, unlike cash, contains within each transaction a verifiable history of its prior transactions.

Implementations differ, but in general a cryptocurrency carries a history of proofs-of-work, which are the earnings statements from which the units of currency at hand, emerged.

In spite of its name, a cryptocurrency is not inherently anonymous. Rather, these currencies, or commodities as they are sometimes classified, use the mathematical techniques of cryptography to embed historical transaction information in such a way that it cannot trivially be altered.

2. What is Bitcoin?

For our purposes, BitCoin was invented by a gentleman named Satoshi Nakamoto,
whose identity is not known, when he described it in the following paper:

BitCoin: A Peer-to-Peer Electronic Cash System.

The presentation is straightforward and may be obtained from www.bitcoin.info. What follows next, are a few notes in summary of the paper, reading this closely, to present some key ideas.

The phrase "peer-to-peer" appears in Nakamoto's title.

Peer-to-peer is a term from computer science. From a cruising altitude of 10,000

feet, we may summarize it as a computer network, in general construed as part of the broader internet, which is not "governed" by a boss computer. Rather, by means of a protocol, i.e. an agreement on how to interact, the system "peers" may be said to police themselves without recourse to a non-peer authority.

"Governed" and "peers" appear in quotes because they describe interactions at one degree of metaphoricity: this system remains governable by external law.

Finance, without cryptocurrency.

Nakamoto writes clearly and we may quote him. Here he describes the world prior
to Bitcoin, or by extension, before cryptocurrency more generally. In fact, there existed cryptocurrency research prior to Bitcoin, of which that paper is a part.

We may think of Nakamoto as offering a critique: of cash, certainly, but further, of the credit card system, with which he is dissatisfied, as becomes evident:

> Merchants must be wary of their customers, hassling them for more information
> than they would otherwise need. A certain percentage of fraud is accepted as
> unavoidable. These costs and payment uncertainties can be avoided in person by
> using physical currency, but no mechanism exists to make payments over a
> communications channel without a trusted party.

Nakamoto is proposing to send "physical currency" over the wire without a designated best-government supervisor or a bank. Enter Bitcoin.

In the Bitcoin paper, Nakamoto goes on to outline for the first time a working

and complete alternative, and name this BitCoin, combining the terms for two minute and similar things: coins, or small quantities of cash; and bits, or small quantities of computer memory.

The paper lingered unaddressed on an email list for some time, later coming to be understood as rather visionary, as it describes how all this could work:

> What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.

What Nakamoto describes as cryptographic proof is what we have referred to previously, and again below, as "proof-of-work."

Nakamoto is invoking a subfield of computer science known as cryptography: the
process of enciphering a message at one end and deciphering it at the other.

Reliance on encryption.

Encryption with computers is possible because certain means of enciphering (or "encrypting") a message is much easier to execute with a computer which is in possession of a mathematical key, then to decipher, whether with or without a computer, without the corresponding key (by brute force techniques or stealth).

Again, it is not so much the keeping-secret of a transactional record that is of interest here to the Bitcoin system, as the difficulty-of-forgery of that transactional record.

Restating: the presence of cryptography is not itself enough to make a

transaction anonymous. Here it is used instead to render the list of transactions unforgeable, or at least, difficult to forge. By analogy then, encryption serves the same purpose as securing the printing plates at a mint.

Encryption as verification.

Nakamoto, in an important section and the last we will quote, describes at a high level of abstraction what he has invented to address this trust problem -- a mechanism which is by now known as blockchain.

Here, Nakamoto refers to something called the double-spending problem. This is the potential for using the same currency to make (e.g.) two transactions, effectively multiplying its value.

Note that the double-spending problem seems not to exist with cash, which is physically transferred from buyer to seller, excepting slight-of-hand, etc.

> Transactions that are computationally impractical to reverse would protect sellers from fraud [Nakamoto, elided, suggests additional technology would be helpful to likewise protect buyers]. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions.

By now Nakamoto is describing the Bitcoin public blockchain.

3. What is blockchain?

The blockchain is a series of cryptographic hashes -- with information about prior transactions in a series. In cryptography, minute changes to an input will result in substantial and easily visible changes to an output.

Because each cryptographic hash relies on the hashes that came before it in the chain, this chain of hashed "blocks" implies a knowledge of all the transactions that came before it.

This linked series of hashed blocks is therefore known as a blockchain.

Without its blockchain and the associated rules, Bitcoin would not work.

4. What can it be used for?

Good question.

Obviously, you can use it to buy and sell Bitcoins or if you prefer, some unrelated cryptocurrency. This is a use case that has people excited.

Likewise, there are implications that follow from technological decisions.

Because blockchain implies an in-general-verifiable history of transactions, cryptocurrencies including Bitcoin, and blockchain generally, have generated some talk about how to use bits and pieces of the tech to do other things.

One way to do that, is to disassemble the public rules that make up the public Bitcoin blockchain, and set them up in a more private setting. This has been proposed elsewhere. By changing the rules of transaction, and perhaps e.g. enforcing honesty by other means, one could use blockchain without Bitcoin.

Another use case is simply building a better mousetrap. Bitcoin and other cryptocurrencies make sub-penny transactions plausible and perhaps profitable.

5. Who can use it?

Anyone with a working computer can in principle use Bitcoin.

6. How can I use it?

The canonical way to get started is to run the software on your computer, installing what is publicly available. Links follow at the end of the pamphlet.

Doing so -- installing what has been provided -- ought to make you a Bitcoin miner, attempting to earn coins through cryptographic proof-of-work, and so, set you on your way.

It should be noted that the cryptographic hashes in Bitcoin imply a public and a corresponding private key. The private keys are only as private as the piece of paper or computer that holds them, and this hold implies control of an asset.

Alternately, you could start a company that deals in one of these currencies. You could build a better "wallet", to hold the private keys, or, start a mining company to generate currency in exchange for expenditures in computing power, maintenance, and electricity. You could speculate directly, in that manner.

Or you could design support components for a given currency, like specialized chips that are good at mining a certain coin.

Extra bits:

Another way to proceed is simply to acquire your coins from someone else. Sell something and accept Bitcoin as a form of payment.

Bitcoin is a speculative commodity which fluctuates in value, so essentially you're buying these at a given rate in hopes of one day exchanging them at, speaking generally, the purchase rate or better.

Bitcoin and its value is tracked, as any other commodity, so you could participate by simply tracking them for a portfolio. So too, with other cryptocurrency, dogecoin, or litecoin, or whatever others you may have heard about. There are quite a number of contenders by now.

With each of these currencies, rules vary, trust varies, liquidity varies.

It's worth noting that there are also government and industry players who are interested in developing technologies, built on blockchain or blockhain-styled systems, which are not currency-related at all. At its heart, blockchain is an enabling technology, a piece of intellectual property and software or systems design which is in the public domain.

So, there are some financial players who hope to use either the enabling ideas or simply the mystique of blockchain, separate from Bitcoin, simply because it's a pretty clever idea.

For example, credit card processors may wish to deploy a technology that uses blockchain techniques for accounting, but not actually the rules of a public blockchain -- something closed and proprietary, or even, open in source, but closed in participation.

This makes cornering the market at least seem a little easier, since you're determining who gets to play and at what level.

A use case might be, to build a closed system that enables clearer sub-penny

transactions; or to provide sovereign-currency to sovereign-currency transfers -- or cryptocurrency to sovereign-currency transfers -- or anything you wish -- at a competitive rate.

You may wish to improve the enforceability of transactions; or to obfuscate them and provide better privacy around individuals. The regulations are in general known but also developing. The money is there. The options are yours.

These are some known ideas about what blockchain, cryptocurrency, and Bitcoin more particularly, may be able to do for you.

This concludes our presentation, with links to follow.

Thanks for reading.

Alex Didek, and,
Alfred S. Matthews

References:

Bitcoin source

https://github.com/bitcoin/bitcoin (https://bitcoin.org/en/download)

Books

Digital Gold: Bitcoin and the inside story of the misfits and millionaires trying to reinvent money; Nathaniel Popper; ISBN 0062362496

Papers, via http://www.bitcoin.info

A-Gentle-Introduction-To-Bitcoin
A-Gentle-Introduction-To-Blockchain-Technology
A-Gentle-Introduction-To-Bitcoin-Mining
A-Gentle-Introduction-To-Digital-Tokens
BitCoin: A Peer-to-Peer Electronic Cash System
Darkcoin Whitepaper
Bitter-to-Better-How-to-Make-Bitcoin-a-Better-Currency
From-Blockchain-Hype-to-a-Real-Business-Case-for-Financial-Markets
Using Blockchain to Boost Commerce

Wikipedia

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

Copyright statement:

Produced on assignment under an Upwork (TM) contract for Alex Didek.

Author (C) 2016, Alfred S. Matthews asm13243546@gmail.com, where applicable.

Released by the author, pending permission, under Creative Commons 2.0: Attribution.