The Crypto Anarchist Manifesto

Timothy C. Maytcmay 1988

Originale:
https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html

Uno spettro sta infestando il mondo moderno, lo spettro della cripto-anarchia.

La tecnologia informatica è sul punto di fornire la capacità agli individui e ai gruppi di comunicare e interagire tra loro in modo totalmente anonimo. Due persone possono scambiarsi messaggi, condurre affari e negoziare contratti elettronici senza mai conoscere il vero nome, o identità legale, dell'altro. Le interazioni sulle reti saranno irrintracciabili, attraverso un esteso reindirizzamento di pacchetti criptati e scatole a prova di manomissione che implementano protocolli crittografici con una garanzia quasi perfetta contro qualsiasi manomissione.
Le reputazioni saranno di importanza centrale, molto più importanti nelle transazioni persino delle valutazioni di credito di oggi. Questi sviluppi altereranno completamente la natura della regolamentazione del governo, la capacità di tassare e controllare le interazioni economiche, la capacità di tenere segrete le informazioni, e altereranno persino la natura della fiducia e della reputazione.

La tecnologia per questa rivoluzione — e sicuramente sarà una rivoluzione sia sociale che economica — esiste in teoria da un decennio. I metodi si basano sulla crittografia a chiave pubblica, sui sistemi di prova interattiva a conoscenza zero e su vari protocolli software per l'interazione, l'autenticazione e la verifica.
L'attenzione è stata finora concentrata su conferenze accademiche in Europa e negli Stati Uniti, conferenze monitorate da vicino dalla National Security Agency. Ma solo recentemente le reti di computer e i personal computer hanno raggiunto una velocità sufficiente a rendere le idee praticamente realizzabili. E i prossimi dieci anni porteranno abbastanza velocità in più da rendere le idee economicamente fattibili ed essenzialmente inarrestabili. Reti ad alta velocità, ISDN, scatole a prova di manomissione, carte intelligenti, satelliti, trasmettitori in banda Ku, personal computer multi-MIPS, e chip di crittografia ora in sviluppo saranno alcune delle tecnologie abilitanti.

5

Lo Stato cercherà naturalmente di rallentare o fermare la diffusione di questa tecnologia, citando preoccupazioni per la sicurezza nazionale, l'uso della tecnologia da parte di trafficanti di droga ed evasori fiscali, e la paura della disintegrazione della società. Molte di queste preoccupazioni saranno valide; la cripto-anarchia permetterà ai segreti nazionali di essere scambiati liberamente e permetterà il commercio di materiali illeciti e rubati. Un mercato anonimo computerizzato renderà perfino possibili abominevoli mercati di assassinii ed estorsioni. Vari elementi criminali e stranieri saranno utenti attivi di CryptoNet. Ma questo non fermerà la diffusione della cripto-anarchia.

Proprio come la tecnologia della stampa ha alterato e ridotto il potere delle corporazioni medievali e la struttura del potere sociale, così anche i metodi criptologici altereranno fondamentalmente la natura delle corporazioni e dell'interferenza del governo nelle transazioni economiche. Combinata con i mercati emergenti dell'informazione, la cripto-anarchia creerà un mercato liquido per qualsiasi materiale che può essere messo in parole e immagini. E proprio come un'invenzione apparentemente minore come il filo spinato ha reso possibile la recinzione di vasti ranch e fattorie, alterando così per sempre i concetti di terra e diritti di proprietà nel Far West, così anche la scoperta apparentemente minore di un ramo arcano della matematica diventerà il tagliafili che smantella il filo spinato intorno alla proprietà intellettuale.

Insorgete, non avete nulla da perdere se non le vostre recinzioni di filo spinato!