CrushCrypto

The History of Digital Currency

Educational Series

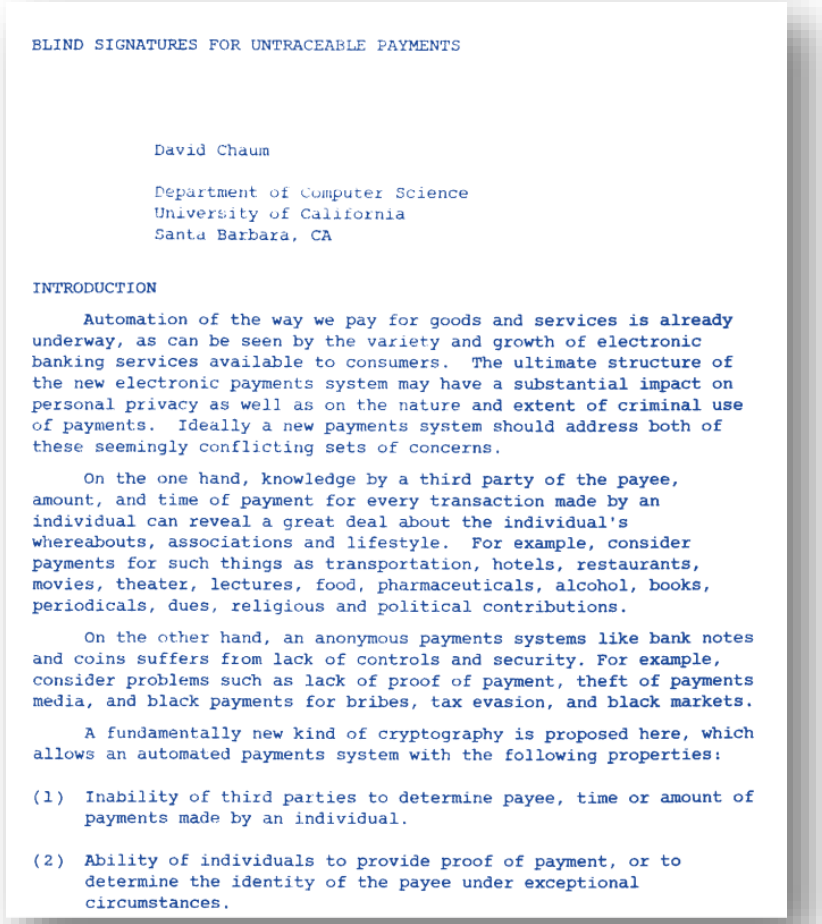
November 26, 2018

Digital Currency Before Bitcoin

- The creation of Bitcoin in 2009 marked the birth of the first digital currency to achieve widespread adoption across the globe. However, the concept of a secure digital currency has been around since the 1980s.
- Previous attempts that inspired Satoshi Nakamoto's creation of Bitcoin include:
    - DigiCash
    - Bit Gold
    - Hashcash
    - B-money

DigiCash

- Computer scientist David Chaum released the paper **Blind Signatures for Untraceable Payments** (1982) in which he outlined an alternative to the electronic transactions hitting retail stores at the time. His paper is considered one of the first proposals of digital currency in history.
- He continued working on his proposal and eventually launched a company called DigiCash in 1990 to commercialize the ideas in his research. In 1994 the company put forth their first electronic cash transaction over the internet.



BLIND SIGNATURES FOR UNTRACEABLE PAYMENTS

David Chaum

Department of Computer Science
University of California
Santa Barbara, CA

INTRODUCTION

Automation of the way we pay for goods and services is already underway, as can be seen by the variety and growth of electronic banking services available to consumers. The ultimate structure of the new electronic payments system may have a substantial impact on personal privacy as well as on the nature and extent of criminal use of payments. Ideally a new payments system should address both of these seemingly conflicting sets of concerns.

On the one hand, knowledge by a third party of the payee, amount, and time of payment for every transaction made by an individual can reveal a great deal about the individual's whereabouts, associations and lifestyle. For example, consider payments for such things as transportation, hotels, restaurants, movies, theater, lectures, food, pharmaceuticals, alcohol, books, periodicals, dues, religious and political contributions.

On the other hand, an anonymous payments systems like bank notes and coins suffers from lack of controls and security. For example, consider problems such as lack of proof of payment, theft of payments media, and black payments for bribes, tax evasion, and black markets.

A fundamentally new kind of cryptography is proposed here, which allows an automated payments system with the following properties:

(1) Inability of third parties to determine payee, time or amount of payments made by an individual.

(2) Ability of individuals to provide proof of payment, or to determine the identity of the payee under exceptional circumstances.

DigiCash (continued)

- DigiCash transactions were unique for the time considering their use of protocols like blind signatures and public key cryptography to enable anonymity. As a result, third parties were prevented from accessing personal information through the online transactions.

- Despite the novel technology, DigiCash was not profitable as a company and filed a chapter 11 bankruptcy in 1998 before being sold for assets in 2002.
- Chaum thought that DigiCash entered the market before e-commerce was fully integrated with the internet and that lead to a chicken-and-egg problem. In a 1999 interview he stated, “It was hard to get enough merchants to accept it, so that you could get enough consumers to use it, or vice versa”.

Bit Gold

- Bit Gold was an attempt to create a decentralized digital currency proposed by Nick Szabo – a computer scientist and cryptographer who is widely regarded as the inventor of smart contracts. Bit Gold was never actually implemented but is considered a direct precursor to Bitcoin considering the technical similarities.
- Szabo did not like the fact that traditional financial systems required a large amount of trust to conduct transactions, leading to issues like fraud and theft. Bit Gold was conceived to provide a more trustless model of transacting, based on the economic properties of gold with increased security.

Bit Gold (continued)

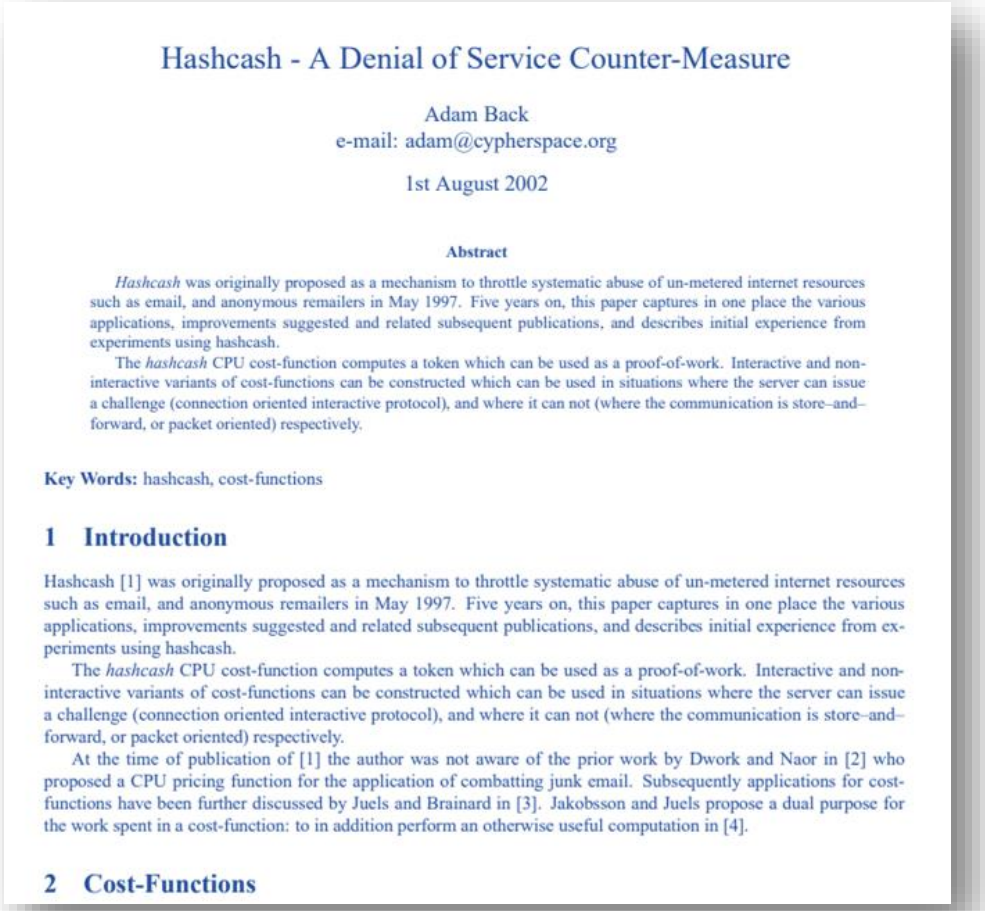
- Bit Gold and Bitcoin are similar because Bit Gold planned to implement a proof-of-work style consensus mechanism where computing power is used to solve cryptographic puzzles. The solved puzzles would then be sent to a Byzantine fault tolerant P2P network with each puzzle attached to the public key of the solver.
- A cryptographic hash would then be used to link the solution of the most recent puzzle to the next puzzle. This method was designed to secure groups of transactions because network users would have to agree on previous puzzle solutions before being able to solve new ones.
- The biggest difference between the proposal for Bit Gold and Bitcoin is the fact that Bitcoin successfully solved the double spending problem.

Bit Gold (continued)

- Most forms of digital currency use a central authority that tracks account balances to combat the double spending issue, but Szabo wanted to mimic the security and trust characteristics of gold, which doesn't depend on a central authority.
- The Big Gold proposal planned to use a Byzantine fault tolerant method relying on a quorum of network addresses, but that made the network vulnerable to Sybil attacks (an attack where one party controls many nodes and manipulates the network).
- Bitcoin utilizes blockchain technology and the concept of block confirmations to enable protection against double spending, allowing for more transaction security than what Bit Gold proposed.

Hashcash

- Initially proposed in 1997 by British cryptographer Adam Back as a “mechanism to throttle systematic abuse of un-metered internet resources such as email”.
- He further detailed the idea in a paper titled **Hashcash – A Denial of Service Counter-Measure** (2002).
- The problem Hashcash aimed to solve was the widespread distribution of spam email. Back’s solution was to require the sender of an email to use a small amount of CPU power to solve a puzzle before sending the email out.



Hashcash - A Denial of Service Counter-Measure

Adam Back
e-mail: adam@cypherspace.org

1st August 2002

Abstract

Hashcash was originally proposed as a mechanism to throttle systematic abuse of un-metered internet resources such as email, and anonymous remailers in May 1997. Five years on, this paper captures in one place the various applications, improvements suggested and related subsequent publications, and describes initial experience from experiments using hashcash.

The *hashcash* CPU cost-function computes a token which can be used as a proof-of-work. Interactive and non-interactive variants of cost-functions can be constructed which can be used in situations where the server can issue a challenge (connection oriented interactive protocol), and where it can not (where the communication is store–and–forward, or packet oriented) respectively.

Key Words: hashcash, cost-functions

1 Introduction

Hashcash [1] was originally proposed as a mechanism to throttle systematic abuse of un-metered internet resources such as email, and anonymous remailers in May 1997. Five years on, this paper captures in one place the various applications, improvements suggested and related subsequent publications, and describes initial experience from experiments using hashcash.

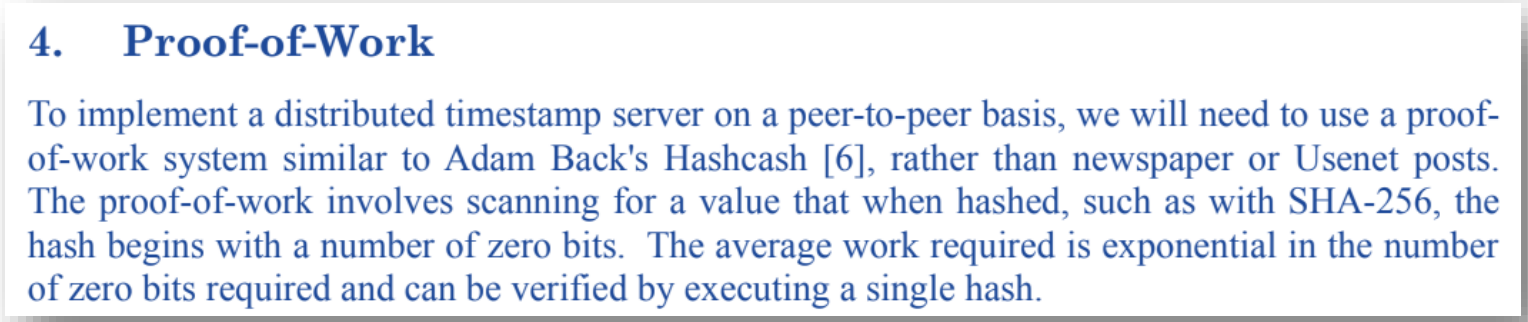
The *hashcash* CPU cost-function computes a token which can be used as a proof-of-work. Interactive and non-interactive variants of cost-functions can be constructed which can be used in situations where the server can issue a challenge (connection oriented interactive protocol), and where it can not (where the communication is store–and–forward, or packet oriented) respectively.

At the time of publication of [1] the author was not aware of the prior work by Dwork and Naor in [2] who proposed a CPU pricing function for the application of combatting junk email. Subsequently applications for cost-functions have been further discussed by Juels and Brainard in [3]. Jakobsson and Juels propose a dual purpose for the work spent in a cost-function: to in addition perform an otherwise useful computation in [4].

2 Cost-Functions

Hashcash (continued)

- For a regular email user, this small amount of CPU power is negligible and in the worst case might delay the sending of an email by a few seconds.
- However, for a spammer trying to send out thousands of emails per minute, the combined CPU power required for each email is significant enough to make this act impossible. The spammer would also have to pay the sum of the electricity costs associated with the required computations if they continued sending out spam.
- Satoshi Nakamoto referenced Hashcash in the Bitcoin Whitepaper:

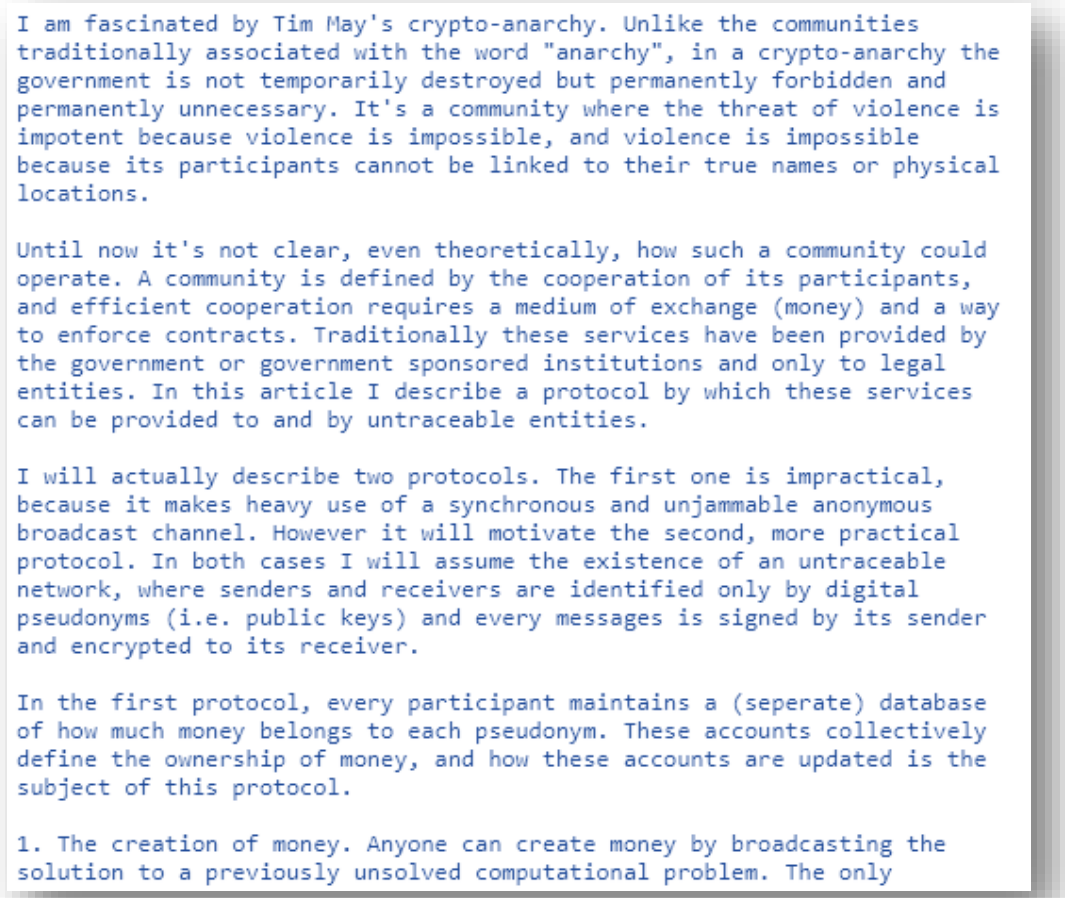


4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

B-money

- B-money was a proposal for an “anonymous, distributed electronic cash system” created by computer engineer Wei Dai in 1998.
- Dai wrote an essay in 1998 outlining his idea and sent it out to the cypherpunks mailing-list.
- In his essay, Dai proposed two protocols, the first of which he knew was impractical because it required “heavy use of a synchronous and un-jammable anonymous broadcast channel” but would serve as motivation for the second protocol.



I am fascinated by Tim May's crypto-anarchy. Unlike the communities traditionally associated with the word "anarchy", in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations.

Until now it's not clear, even theoretically, how such a community could operate. A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) and a way to enforce contracts. Traditionally these services have been provided by the government or government sponsored institutions and only to legal entities. In this article I describe a protocol by which these services can be provided to and by untraceable entities.

I will actually describe two protocols. The first one is impractical, because it makes heavy use of a synchronous and unjammable anonymous broadcast channel. However it will motivate the second, more practical protocol. In both cases I will assume the existence of an untraceable network, where senders and receivers are identified only by digital pseudonyms (i.e. public keys) and every messages is signed by its sender and encrypted to its receiver.

In the first protocol, every participant maintains a (seperate) database of how much money belongs to each pseudonym. These accounts collectively define the ownership of money, and how these accounts are updated is the subject of this protocol.

1. The creation of money. Anyone can create money by broadcasting the solution to a previously unsolved computational problem. The only

B-money (continued)

- In the first protocol, a proof of work function is suggested as a way to create money, proposed as a possible application of Hashcash's proof of work technology as mentioned earlier.
- Also, transactions would be broadcasted to all network participants and everyone would keep track of how much money belongs to each account. Dai then outlined the possibility of contracts that could be made with reparation in case of default, and a third party as an agreed arbitrator.

B-money (continued)

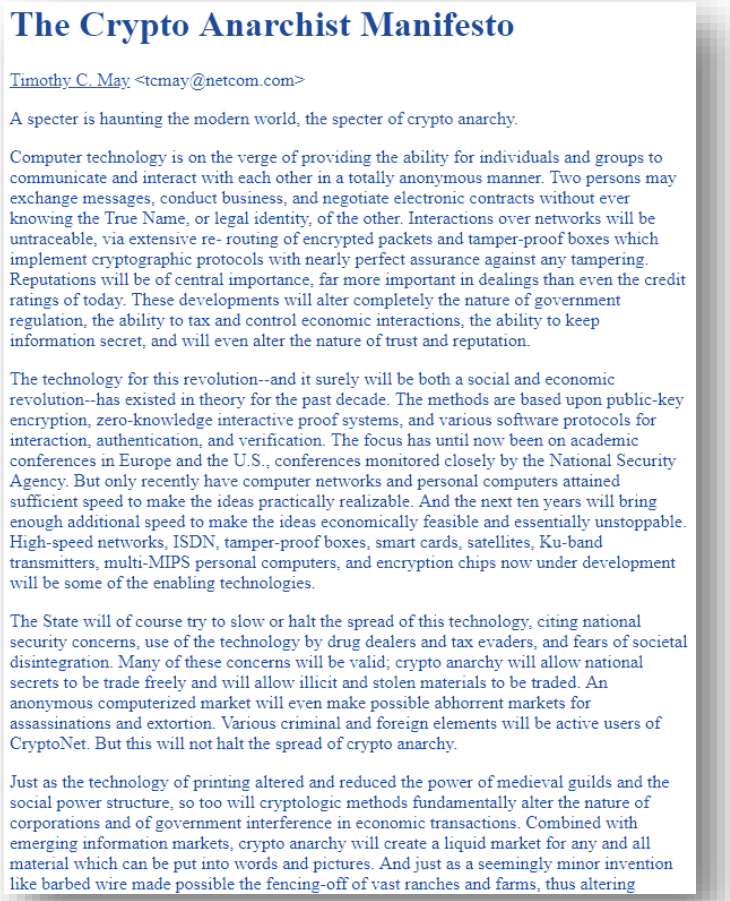
- The second protocol was different from the first because only a subset of network participants (servers) are used to keep track of how much money is owned by each account.
- Considering the servers must be trusted, Dai wrote that a mechanism to keep them honest is required. His idea was to have each server deposit a certain amount of money in a special account to be used for potential fines or rewards for proof of misconduct.
- The format of transactions broadcasted on the network was the same as described in the first protocol, with the added expectation that transaction participants would verify the message has been received and processed by a randomly selected subset of the servers.

Cypherpunks and Stateless Currency

- **Cypherpunks** are a collection of activists that advocate for the use of privacy-enhancing technologies such as cryptography for social and political change.
- In 1992 Eric Hughes, Timothy C. May, and John Gilmore founded a small group of cryptographers that would meet in person in San Francisco and adopted the name “Cypherpunks”.
- The Cypherpunks mailing list was created in the same year as an active forum for technical discussion on topics like cryptography, math, computer science, politics, and philosophy.

Cypherpunks and Stateless Currency (continued)

- Cypherpunks generally hold Libertarian political views and many believe in the idea of crypto-anarchism outlined in Timothy C. May's **The Crypto Anarchist Manifesto** (1992).
- May mentions that new technologies "will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation."
- He also states that the technology for this social and economic revolution has existed in theory since the 1980's, but "the next ten years will bring enough additional speed to make the ideas economically feasible and essentially unstoppable."



The Crypto Anarchist Manifesto

Timothy C. May <tcmay@netcom.com>

A specter is haunting the modern world, the specter of crypto anarchy.

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re- routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.

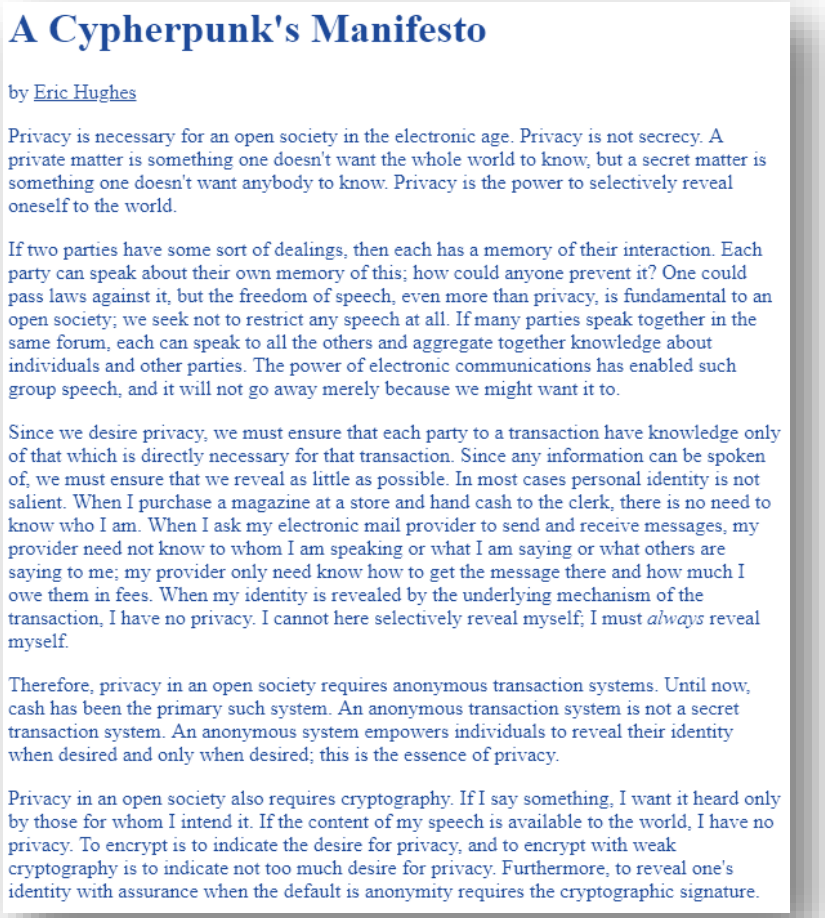
The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. The focus has until now been on academic conferences in Europe and the U.S., conferences monitored closely by the National Security Agency. But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable. And the next ten years will bring enough additional speed to make the ideas economically feasible and essentially unstoppable. High-speed networks, ISDN, tamper-proof boxes, smart cards, satellites, Ku-band transmitters, multi-MIPS personal computers, and encryption chips now under development will be some of the enabling technologies.

The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.

Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering

Cypherpunks and Stateless Currency (continued)

- In 1993, Eric Hughes released **A Cypherpunk's Manifesto** which outlined the core principles of the Cypherpunk movement.
- Key statements include:
  - Privacy is necessary for an open society in the electronic age.
  - Privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system.
  - Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it.



A Cypherpunk's Manifesto

by Eric Hughes

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

If two parties have some sort of dealings, then each has a memory of their interaction. Each party can speak about their own memory of this; how could anyone prevent it? One could pass laws against it, but the freedom of speech, even more than privacy, is fundamental to an open society; we seek not to restrict any speech at all. If many parties speak together in the same forum, each can speak to all the others and aggregate together knowledge about individuals and other parties. The power of electronic communications has enabled such group speech, and it will not go away merely because we might want it to.

Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. Since any information can be spoken of, we must ensure that we reveal as little as possible. In most cases personal identity is not salient. When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others are saying to me; my provider only need know how to get the message there and how much I owe them in fees. When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must *always* reveal myself.

Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.

Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available to the world, I have no privacy. To encrypt is to indicate the desire for privacy, and to encrypt with weak cryptography is to indicate not too much desire for privacy. Furthermore, to reveal one's identity with assurance when the default is anonymity requires the cryptographic signature.

Cypherpunks and Stateless Currency (continued)

- The Cypherpunks mission is to build open source systems designed to defend privacy for everyone in this technological era. They believe that individuals should have the power to reveal their identity and words only when desired, and that neither governments nor corporations can sufficiently protect this right.
- The Cypherpunk movement is directly responsible for the creation of digital currency, blockchain technology, and Bitcoin. All four founders of the Bitcoin precursors mentioned above (Adam Back, Nick Szabo, Wei Dai, and David Chaum) were Cypherpunks that first proposed their ideas through the mailing list.
- Satoshi Nakamoto cited a number of Cypherpunks in the Bitcoin whitepaper, and first announced the whitepaper and genesis block creation through the mailing list. Additionally, many of the early Cypherpunks became core developers for Bitcoin including Hal Finney and Adam Back.

CrushCrypto