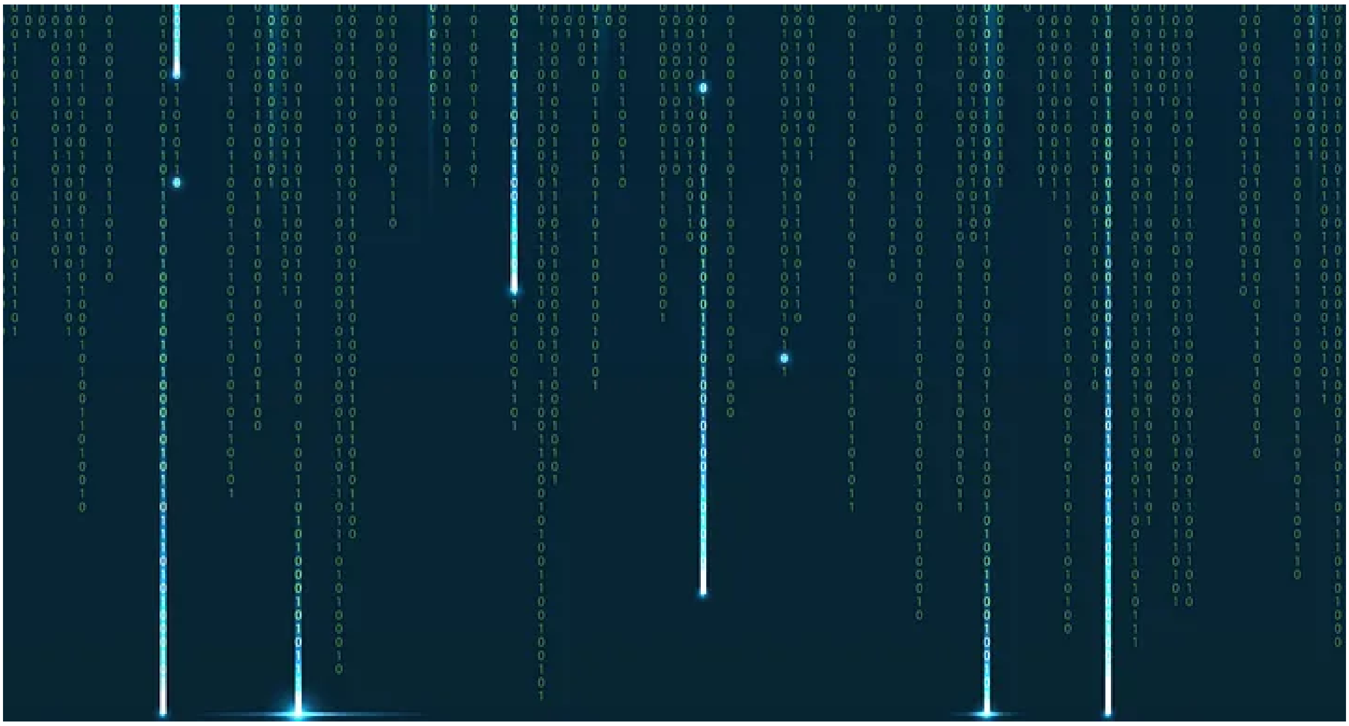
The untold history of Bitcoin: Enter the Cypherpunks

P3 · Follow

Published in The Startup

5 min read · Jan 26, 2018

Listen Share



In my previous article I addressed the underlying technologies that blockchain runs and the history behind how it all started. The primary focus of that article was the development of PGP encryption by Phil Zimmermann, the wonder of open source software and peer-to-peer networks that are almost impossible to stop.

But how did all the pieces come together to ultimately create what we know today as Bitcoin?

In late 1992, three individuals (Eric Hughes a mathematician from University of California, Berkeley; Tim May, a retired businessman who worked for Intel and;

John Gilmore a computer scientist who was Sunmicrosystems' fifth employee) who had all retired young, invited twenty of their closest friends to an informal meeting to discuss some of the world's seemingly most vexing programming and cryptographic issues.

The Cypherpunks

That initial meeting eventually evolved into a monthly meeting held at John Gilmore's company, Cygnus Solutions. At one of the first meetings, Jude Milhon (a hacker and author better known by her pseudonym St. Jude) described the group as the "Cypherpunks" a play on the word 'cipher' or 'cypher', one of the ways to perform encryption and decryption and; cyberpunk a genre of fiction made popular by sci-fi writers.

From those humble beginnings, an entire movement evolved.

As the group grew it was decided that setting up a mailing list would allow them to reach other "Cypherpunks" outside of the bay area. The mailing list grew in popularity fairly quickly and included hundreds of subscribers who were exchanging ideas, discussing developments, proposing and testing cyphers on a daily basis. These exchanges took place through the use of novel (at the time) encryption methods, such as PGP, to ensure complete privacy. As a result, ideas were shared freely.

This privacy and freedom resulted in free flowing discussions on wide ranging topics from technical ideas such as mathematics, cryptography and computer science to political and philosophical debates. Although there was never complete agreement on any one thing, this was an open forum where personal privacy and personal liberty were ultimately placed above all other considerations.

The basic ideas behind this movement can be found in the Cypherpunk manifesto written by Eric Hughes in 1993. The key principle which underpins the manifesto, is the importance of privacy. One can see this and other principles discussed in the manifesto being used to build the ideas that support some of the largest cryptocurrencies today.

Regarding privacy, the Cypherpunk manifesto says the following:

> "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."

It even goes into very practical examples directly related to day to day transactions:

> "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 …….. 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."

Based on these principles a number of attempts were made to develop digital currencies.

The early attempts

The first attempt at such an anonymous transacting system was made by Dr. Adam Back in 1997 when he created Hashcash. At its essence, this was an anti-spam mechanism which would add a time and computational power cost to sending email, therefore making the sending of spam uneconomical. A sender would have to prove that they had expended computational power to create a stamp in the header of an email (similar to the proof of work (POW) use in Bitcoin) before they were able to send it.

In the following year Wei Dai published a proposal for B-Money. His proposal included two methods of maintaining the transaction data; a) every participant to the network would maintain a separate database of how much money belongs to users and, b) all records are kept by a specific group of users. In the second option the group of users who have custody over the records are incentivised to be honest because they have deposited their own money into a special account and stand to lose it if they are not. This method is known as "proof of stake" (POS) and the specific groups of users (or master nodes) will lose all the funds they have stakes if they attempt to process any fraudulent transaction.

Many crypto currencies are using, or considering moving to, this method of transaction verification due to its efficiency (the most noteworthy being Ethereum (ETH)).

In 2004, Hal Finney created Reusable Proofs of Work which borrowed from the principles of Backs' Hashcash and in 2005 Nick Szabo published a proposal for Bitgold which built on the ideas developed by Hal Finney and various other projects.

As can be seen, various people from across the world have been working tirelessly on the blockchain technology and crypto currencies since the 1990's and there have been multiple attempts to solve the complex issues surrounding cryptocurrency, by arguably some of the most brilliant minds in this space.

Enter Satoshi

In October 2008 Satoshi Nakamoto, an unknown individual or group of individuals, sent a paper to the cypherpunk mailing list at metzdowd.com called: "Bitcoin: A Peer-to-Peer Electronic Cash System". (I highly recommend that you read this paper, its only 9 pages).

The paper made direct references to b-money and hashcash and addressed many of the problems that the earlier developers faced including double spending (the risk that a single token is used multiple times to purchase goods). The paper attracted a lot of criticism from sceptics, but Nakamoto continued on and mined the genesis block of Bitcoin on 3 January 2009.

Since its inception, Bitcoin's development has continued to come under fire by critics and sceptics but "the honey badger" (as it is commonly known) keeps on going.

This story is published in The Startup, Medium's largest entrepreneurship publication followed by 289,682+ people.

Subscribe to receive our top stories here.