From Bitcoin: the Future of Money? by Dominic Frisby

THE ANARCHIC COMPUTING SUBCULTURE IN WHICH BITCOIN HAS ITS ROOTS

Cypherpunks write code.
— Eric Hughes, mathematician and Cypherpunk

In September 1992, Tim May, a computer scientist whose inventions had once made him a great deal of money at Intel, invited a group of eminent, free-thinking programmers to his house in Santa Cruz, California, near Silicon Valley. They were there to discuss this exciting new development called the internet. They were excited about the possibilities, but they were also concerned. Privacy was their issue.

Beyond the realm of cash payments, no transaction is private. And your financial behaviour says more about you than anything. Banks, credit card companies, merchants and – most worryingly for Tim May and his friends – the government would all have access to this information on the internet. How would they use it?

They were scared of Big Brother.

Some of the group simply wanted to find ways to protect privacy, others wanted to fight back. Their mistrust was born of experience. Their friend, the programmer Phil Zimmerman, was under criminal investigation for a simple piece of privacy software he had developed called PGP (Pretty Good Privacy). He was in serious trouble with the US authorities, who said he had violated the Arms Export Control Act.

'Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure', said May that night, 'so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions...just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property. Arise, you have nothing to lose but your barbed wire fences!'

They were a committed, disparate and talented group of computer scientists. Their belief system was largely libertarian; they understood the potential of the internet, but they also saw the possibilities it was opening up for state and corporate invasion of privacy. They thought cryptography could lead to social and political change. By the end of the meeting, an anarchist philosophy had been born, that of the Cypherpunks.

Within a week mathematician Eric Hughes, a co-founder of the movement, had written a programme that could receive encrypted emails, remove any signs by

which they could be identified and send them out to a list of subscribers. Now they had the Cypherpunks Mailing List. On this email list, they would share, discuss and develop their ideas.

When you signed up, you were greeted with a message from Hughes: 'Cypherpunks assume privacy is a good thing and wish there were more of it. Cypherpunks acknowledge that those who want privacy must create it for themselves and not expect governments, corporations, or other large, faceless organizations to grant them privacy out of beneficence'.

That message became the spine of his *Cypherpunk Manifesto*.

"Privacy is the power to selectively reveal oneself to the world. 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...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...If I say something, I want it heard only by those for whom I intend it...We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place...Cypherpunks are therefore devoted to cryptography. Cypherpunks wish to learn about it, to teach it, to implement it, and to make more of it...We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money...Our code is free for all to use, worldwide. The Cypherpunks are actively engaged in making the networks safer for privacy. Let us proceed together apace."

Their mantra, 'Cypherpunks write code', meant that rather than talk about how things should be, they would make things as they should be through computer code. If a system isn't working, write some code and make it work.

The ultimate dream of the movement was a system of digital cash outside the invasive capabilities of governments or banks. Many attempts have since been made. Each one failed.

Until Bitcoin.

From Bitcoin: the Future of Money? by Dominic Frisby

The Cypherpunk Manifesto (LINK TO PDF or https://www.activism.net/cypherpunk/manifesto.html)