A brief overview of Cyberpunks and Cypherpunks movements

By Martin Rupp
SCIENTIFIC AND COMPUTER DEVELOPMENT SCD LTD

Warning: this is a purely historical & neutral approach and linked to cryptographic science history, This doesn't mean that the author exposes any personal political position - in this article - regarding some of the ideas linked to the Cyberpunk movement.

1 Introduction

We want this article to give the readers an interesting and comprehensive overview of a badly known movement which is linking technology, cryptographic and politics, this is the *Cyberpunk* movement.

Cyberpunk is at start an artistic movement and features a dystopian future where life is in general quite hard and where the level of technology is important and especially using cybernetics, robotics and artificial intelligence.

Cyberpunk finds its illustration with movies such as *Blade Runner* and in general with everything adapted from the work of Philip K Dick. *Matrix* or *Ghost in the Shell* are other perfect examples of Cyberpunk movies.

Cyberpunk has several sub-genre such as *Steampunks* or *Gothpunks.* One of these sub-genres is the *Cypherpunk* movement.

2 Cyberpunk, Cypherpunks and computer programming

It is not very well-known that in the 80s the cyberpunk movement gave rise to a culture of programmers which were applying the philosophy of the movement not as artists but as “technological activists". This means that they were really “living" and “acting" the movement by being themselves a *real* part of it.

Of course in general cyberpunk was linked to the culture of computer hacking in terms of programming culture: fighting against mega-corporations, defeating conspiracies or unveiling dark government secrets.

This may sound familiar to you… this is exactly why Julian Assange, the founder of Wikileaks was (and is still more than ever) a part of the cyberpunk culture.

What may surprise you even more is that the Bitcoins and all the actual crypto-values are the fruit of a subgenre of cyberpunk: the cypherpunk movement!

2.1 What is Cypherpunk?

In late 1992, Timothy C May, Eric Hughes, and John Gilmore grouped several people that had monthly meetings at the premises of the company Cygnus Solutions (owned by John Gilmore) and located in the San Francisco Bay Area. That group was coined (humorously) “cypherpunks" from a *portmanteau* of “cipher" and “cyberpunk."

Cypherpunks usually have a desire for the widespread development of strong cryptography for the average person as well as the development of technologies improving privacy as a way to promote social and political changes.

The Cypherpunk ideology advocates anonymity and the use of cryptography to protect citizens against inordinate control from police states such as the one described in the “big brother" book by George Orwell.

2.2 The Cypherpunk manifesto

The manifesto was written by Eric Hughes, an American mathematician, computer programmer and considered to be the main founder of the cypherpunk movement. This is a very brief text based on the necessity to have strong anonymity in the digital area.

Extract of the manifesto:

“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".

As Bruce Schneier has once explained, the “nothing to hide" argument comes from a twisted logic and from the false hypothesis that privacy always involves the hiding of something bad or wrong.

2.3 Cypherpunk and The Bitcoin

In 1997, Dr Adam Back created the Hashcash system, which was merely conceived as an anti-spam mechanism which would essentially add a cost in terms of computations to sending email, thus making spam not interesting.

Later in 1998, Wei Da, a computer engineer known for contributions to cryptography and cryptocurrencies, published a document that described the “b-money" system, a concrete way to enforce agreements in terms of contracts between anonymous actors

In 2004, Hal Finney created the reusable proof of work (RPOW), which was based partially on the Hashcash

Nick Szabo, a computer scientist, legal scholar and cryptographer known for his research in digital contracts, published a proposal for “bit gold" in 2005

Finally, in 2008, Satoshi Nakamoto published the bitcoin whitepaper, quoting both hashcash and b-money.

Bitcoin strengthened the entire cypherpunk movement by allowing cypherpunk organizations to continue their operations via bitcoin donations, even if the banking system had blacklisted them.

3 Cypherpunk leading the quest for anonymity

Cypherpunks lead the way when it comes to anonymity in the digital age. Their work with Tor, the onion router or with the remailer systems is legendary.

Cypherpunks have also done a lot of work in systems designed to improve strong anonymity in digital currencies. For example the development of systems that can prevent the blockchain Observers to be opponents to anonymity. Darksend+ and Darkcoin were developed by cypherpunks.

4 Cypherpunks and the EEF

The EEF, the Electronic Frontier Foundation is an important nongovernmental organization which aims at protecting the users of the internet - and in general cyberspace - from abuses. The EEF is often linked to Cypherpunks which are also strong cryptographers. For example the DES breaking machine (“Deep Crack") was designed partly by Cypherpunks.
Recall that Cypherpunks are not usually hackers but seek to prove the limits and danger of governmental-based cryptography and advocate a free usage of cryptography. Therefore, they demonstrated with success that the official US standard in terms of cryptography, the DES, was in fact very vulnerable to attacks, at the time, in 1998.

5 Cypherpunks and the ‘Anonymous’ organization

There is obviously a link between the Cypherpunk movement and the organization of ‘Anonymous’ but while Cypherpunks do not recommend illegal actions, the ‘anonymous’ organization is clearly based on hacking and illegal intrusion in remote computer systems.

Anyway Cypherpunks and the ‘Anonymous’ organization share a common ground, the ground of crypto-activism and crypto-anarchism.

6 list of famous Cypherpunk people

Here are some famous Cypherpunks (source: Wikipedia):

- Jacob Appelbaum: Tor developer
- Dr Adam Back: Inventor of the Hashcash and co-founder of Blockstream
- Bram Cohen: The Creator of BitTorrent
- Hal Finney: ONE of the main authors of PGP 2.0 and the creator of the Reusable Proof of Work
- Tim Hudson: Co-author of SSLeay
- Paul Kocher: Co-author of SSL 3.0
- Moxie Marlinspike: The founder of Open Whisper Systems
- Steven Schear: Developer of the concept of the “warrant canary"
- Bruce Schneier: A famous security author
- Zooko Wilcox-O’Hearn:The founder of Zcash

- Philip Zimmermann: The creator of PGP 1.0

7 Conclusion

Cypherpunks are part of every day's life in computer systems but the "general public" is usually ignorant of that fact. Using Tor, ProtonMail, the Bitcoin or similar tools may seem banal but without the Cypherpunk movement, such tools would have never been created. Some aspects of the Cypherpunk movement will be 'controversial' by nature but most of the anonymity that we are using now in cyberspace comes from their activism and research.