Privacy is not secrecy.

Privacy is the power to selectively
reveal oneself to the world.

We must defend our own privacy
if we expect to have any.

Cypherpunks, Crypto-Anarchism, and the Future of Privacy

A Primer

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.

By 4NTS Guild

Cypherpunks write code.

Privacy only extends so far as the cooperation
of one's fellows in society.

Onward.

4NTS

Introduction

Technology is a value-laden discipline integrated with other aspects of social and political life. Technological developments contribute to sustaining certain views of the world, open up new paths for growth, and envision new ways of establishing relations with our surroundings.

It is fundamental to acknowledge the political and social character of technology and gain an awareness of the political and social role that technologies such as distributed ledger technology are going to play. For that, it is necessary to reflect both on the political ideas that have triggered the birth of distributed ledger technology (DLT), and also how its design aligns with them.

The Ideological Foundations of Bitcoin, DLT, and the Open Web

Distributed ledger technology emerged in the manifestation of Bitcoin, from the joint effort of cypherpunks and crypto-anarchists. These people envisioned a different future for society, a future free of the violence perpetrated by the State's coercive methods. The open-source design crypto-economic protocols reflects these ideals: As adoption and interest increases, the underlying ideals for such ecosystems are positioned to emerge further.

Unfortunately, there are many misconceptions surrounding the cypherpunk movement as well as crypto-anarchists. In this paper, we explore the political and philosophical ideas that have nurtured the cypherpunks and crypto-anarchists in order to dispel the misconceptions surrounding them. This endeavour will not only enable us to better understand DLT technology, but also to show how - through Bitcoin and the Open Web - what was once a cypherpunk ideal has found its way into reality.

The word cypherpunk was first coined by hacker Jude Milhon in 1992. To do so, he combined "cypher" (cypher) and "punk" (rebel). Simply put, cypherpunk is "cypher rebels". It refers to activists that contribute to the advancement of cryptographic technology for

defending privacy, and advocate for greater freedom of expression. The word has an earlier, well-known derivation, that of cyberpunk. This word is used to define a futuristic, science fiction, dystopian literary genre in which technology is central to the plot. The word should also not be confused with crypto-politics as crypto-politics simply refers to the secret support of a political belief. It thus has nothing to do with cypherpunks.

Cypherpunks and Crypto-anarchists: Tracing the History of DLT

Blockchain made its public appearance in 2008 when Satoshi Nakamoto inaugurated Bitcoin. Its genesis can be traced back to the cypherpunk movement, a movement that advocates for greater privacy, limited government involvement, and freedom of speech.

Timothy C. May in the documentary *Cypherpunks Write Code* (watch here)

The cypherpunk movement was born at the end of the 80s and was initiated by Eric Hughes, Timothy C. May, and John Gilmore. Inaugurated by Timothy May's Crypto-Anarchist's Manifesto, the cypherpunk movement focuses on privacy issues on the open web, defining privacy as: "the power to selectively reveal oneself to the world"(Hughes, ed. Ludlaw, 2001, p. 81). Their main goal is then to prevent the revealing of unnecessary information that is commonly required by transactions. As Hughes writes:

"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. Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it […]. Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation's border and the arm of its violence. Cryptography will ineluctably spread over the whole globe and with it the anonymous transactions systems that it makes possible" (May, ed. Ludlaw, 2001, p. 83*).*

The cypherpunk movement originated as a reaction to growing State interference on the private life of citizens facilitated by digitalisation. The control of sensitive information by the government is seen as a dangerous liability for citizens and as a significant breach of their right to freedom. The cypherpunk movement wants to reverse this state of affairs by creating the means to retain control of personal information at all times. They are firm supporters of the freedom of speech which they protect through anonymity and pseudonyms. They stand in opposition to any governmental policy that attempts to control and limit the use of cryptography.

Cypherpunks have fought several battles against the U.S government, namely by filing lawsuits against it for its attempts to limit cryptography and also by inciting civil unrest. While many of their achievements continued to be hampered by the government, some of their accomplishments such as MintChip, Canadian e-wallet, and Bitcoin, could not be restrained - and continue to not only exist - but thrive.

"Cypherpunks are advocates for the widespread use of strong cryptography and privacy-enhancing technologies. Cypherpunks invented/created the EFF, PGP, SSL, SSH, BitTorrent, Tor, WikiLeaks, Bitcoin, smart contracts, Zcash, and Signal, among other notable achievements."

Crypto-anarchism is another important movement developed by the early cypherpunks. While retaining the same principles of the cypherpunk movement, crypto-anarchism frames itself as a more encompassing political movement. As the name suggests, crypto-anarchism proposes to overcome the purview of traditional nation states and found a society based on freedom of association, cooperation, egalitarianism, economic libertarianism, and decentralisation.

According to crypto-anarchism, cryptographic methods will alter the nature of corporations and of government interference in economic and social transactions. As May puts it:

> "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" (May, ed. Ludlaw, 2001, p.62).

Crypto-anarchists are not only committed to building software that can provide protection against State abuses: They also strive to build new socioeconomic structures through computer code.

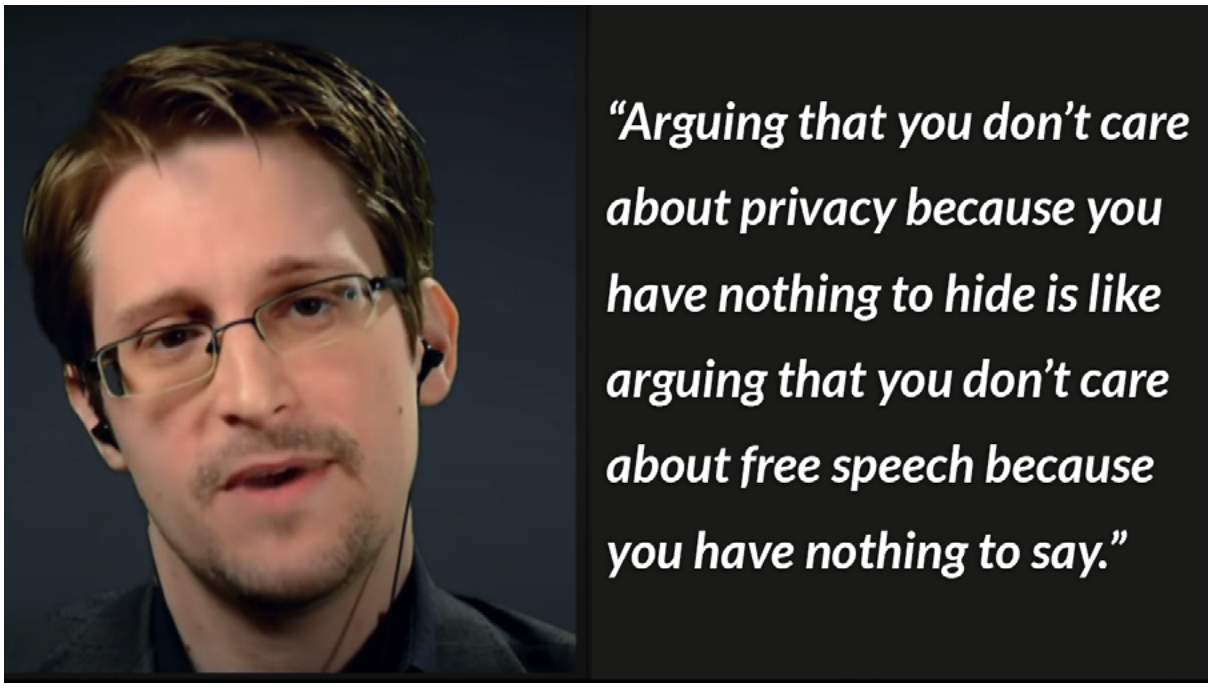
In this context, it is possible to understand how crypto-anarchist ideas and values are reflected in the architecture of DLT. DLT allows a collective of people to formulate, disseminate, maintain and verify an institutional system while recording the interactions within it (MacDonald, Allen and Potts, 2016). It allows us to change the very ways we govern ourselves as collectives and provides the basis for a non-coercive, consensus based society.

Why Does Crypto-Anarchism Matter Today: Surveillance, Money and the State

Today we are forced to deal with economic and political institutions that are expensive and exclusionary: They have a high potential for error and they intrude into users' personal privacy without oversight or accountability. In many ways, such institutions are the key stakeholders of a dystopian world of oppression, in which technology is exclusively managed by the state and massive corporations.

From cypherpunk and crypto-anarchist Frank Braun's Twitter

Yet, the most problematic part is that we are not fully aware of the fact that mass surveillance has become increasingly cheap, invisible, and pervasive. The most popular argument that pops up when someone hears about a loss of privacy is: "But I have nothing to hide, so I don't care". However, privacy is not about hiding the wrong, but rather about having control over one's own communication. In the "nothing to hide" logic, the choice comes down to a passive acceptance of mass surveillance instead of an active defense of one's own rights. For other responses to the '*Nothing to Hide Argument*' see Amnesty's article.



Edward Snowden in the documentary *Nothing To Hide, Nothing To Fear*

Companies like Facebook, Google and Amazon have succeeded in making users' online life more and more comfortable by allowing them to purchase an item within a few minutes, receive relevant information based upon earlier internet surfing, by automatically finding a recognized friend's face on the picture. The downside of such "convenience" is that big corporations and government agencies exploit and often misuse user's private data for personal returns (see Shoshana Zuboff, *The Age of Surveillance Capitalism*).

"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." - The Cypherpunk Manifesto

While technology has undoubtedly become a great asset for boosting our efficiency, we cannot ignore the fact that the power asymmetries that result from the current state of affairs increases users' vulnerability. Hence, the goal is to find an optimal way to deploy technology to serve users' best interests while also ensuring the integrity of the process from start to finish.

Money and State: The Need For Privacy and Autonomy

As previously mentioned, crypto-anarchism is a movement that uses encryption to allow users to exist online anonymously. It strives to free private data from institutional surveillance. “Encryption” is the method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. While encryption can be highly beneficial for individual users, it is often interpreted as a threat to governments and related agencies, who have a vested interest in monitoring communications as well as economic transactions.

At root, the value proposition of encryption is closely related to the structure of the modern financial system and the relationship between governments and financial service providers. While this relationship has evolved over time, the financial crisis of 2007-2008 illustrated the excessive confidence in existing markets efficiency by a number of centralized and ‘too-big-to-fail’ institutions. In the context of the crisis, major banks lent huge volumes of money to one another, while average citizens remained at the mercy of these institutions for accessing, handling and transaction value. As a result of this system, many countries continue to experience the consequences of the - 13 years and running - monetary policy failure.

Austerity, huge debts, increased unemployment and overall political instability , beg the question: What can we learn about the role of the State from this?

To save the economy from failure, governments around the globe have (and continue to) pump billions of dollars into the financial system to rescue national banks. This expansive fiscal policy does not offer a long-term solution to the fundamentally degraded fiscal policy of Central Banks. That is not to say that the government interventions were completely useless, but rather that our (economic) reality today is too complex to be controlled by money alone.

Crypto-anarchism highlights the weaknesses of the current economies when it comes to absorbing shocks and the inability of the states to come up with effective and sustainable solutions. Crypto-anarchism seeks to build an alternative reality where citizens can redefine their economical interactions, strive towards socio-egalitarianism and potentially achieve greater agency.

How The Open Web Realizes The Crypto-Anarchist Ideal

The unique features of DLT match ideally with the main principle of the crypto-anarchist and cypherpunk movements. With its emphasis on security and decentralization, DLT provides a trusted digital space to cultivate independent asset management, user empowerment, autonomy, as well as strong cooperation. Two closely related fields that compliment the crypto-anarchist ideal of freedom and privacy, are (1) Cryptocurrencies and the (2) Deep Web. Since both are full of controversies and are frequently misunderstood, we will attempt to debunk a couple of myths thereof.

Myth 1: Cryptocurrency Is Just Another Currency

One of the major competitive advantages of distributed ledger technology over the state is high security. Historically, institutional systems have developed different ways to record transactions of all kinds. The goal has always been to create a system that would be resilient to theft of information, corruption and manipulation. Today the nexus of power has become hopelessly corrupt and hence the state fails on these premises. We know this because of the digital profiling or detailed pictures of each individual based on the online activity. All big corporations are chasing consumer behavior because they can extract huge value from it.

Cryptocurrencies, as a decentralized peer-to-peer digital system for the exchange of value, offer an alternative model to the current state of art financial instruments, where financial information is controlled and traced by the state and related institutions.

Cryptocurrencies, thus are more than simply another currency. In virtue of being based on public distributed ledgers, they provide a foundation for creating new ways to handle financial data, outside of the reach of surveillance capitalists. This is exactly the reason why cryptocurrencies were so well-received in the crypto-anarchist community and beyond.

From a crypto-anarchist perspective, several DLT applications have the potential to enable self-sustaining economic organisation. Besides control over data, cryptocurrencies offer another, more effective, anti-inflatory economic model. Bitcoin, for instance, grows organically due to the limited number of coins and hence circumvents inflation. Other cryptocurrencies, meanwhile, have been designed to be private, anonymous and fast making them popular in Dark Web markets.

Myth 2: The Dark Web Is For Human-Trafficking And Drug Exploitation

"The dark web is the hidden collective of internet sites only accessible by a specialized web browser. It is used for keeping internet activity anonymous and private, which can be helpful in both legal and illegal applications. While some use it to evade government censorship, it has also been known to be utilized for highly illegal activity. (What Is The Deep Dark Web, 2020)

When the term 'Dark Web' comes up, there is a tendency to assume that only people engaged in illegal activity would want to use it. Contrary to the various stereotypes and biases, the Deep Web is largely composed of safe content like public and private databases and intranets that we use every day. The face of crime has undoubtedly changed with the birth of anonymizing browsers like Tor, but as crypto-anarchists emphasize there is a beneficial side to the hidden internet.

For instance, the Deep Web can be seen as a new, more democratic commercial area. Imagine, that it was not only a place to bypass the local geographical restrictions and watch a local TV but a place where one can buy otherwise unaffordable medicines to treat cancer patients? Can it become another equivalent of eBay?

Realizing the crypto-anarchist dream, the features of the Deep Web accurately represent values such as retention, reciprocity and integrity. An absence of web page indexing and network security like encryption protects users from Google and others accessing their data. Anonymous markets, therefore, should not only exist for drugs but also for food, medicines and more. Prices on the black market have the capacity to make products more accessible.

Most importantly, any understanding of the 'Dark Web' must be mindful of the current context of surveillance and rash disregard for privacy that much of the world lives through today. It is therefore highly appealing to rejuvenate the concept of the Deep Web from the crypto-anarchist angle and explore its potential usability for improving data privacy and building an alternative economic system: We may consider the Dark Web as a means by which users can fight against totalitarianism.

Conclusion

For years cypherpunks and crypto-anarchists have warned us about the dangers of an overtly centralised state apparatus. They have opposed the status quo by developing the technological means to escape surveillance and engaged in overt resistance to state oppression. Their work has been impactful, while, nevertheless, surveillance capitalism continues to thrive at the expense of people's freedom and agency.

In this context, the adoption of a technology that prevents tech giants and the state alike from holding a disproportionate amount of power and information over people becomes crucial in order to safeguard fundamental freedoms, rights and human dignity. Ultimately, the Open Web, and its core underlying distributed ledger technology, have the capacity to ground a pathway towards a society where privacy, freedom, and transparency are provided to its citizens. It is therefore crucial that its development is followed, and encouraged.

In parallel to the development of this technology will allow people greater freedom and autonomy it is also fundamental to raise awareness about the importance of privacy. The implications of corporate and government access to personal data is still not fully understood, as the mainstream narrative surrounding privacy belittles the importance of user's control over their information. Increasing awareness on the importance of privacy is thus also essential for people to realise the necessity and urgency of building an Open Web.

Cypherpunk Reading List and Recommendations

The Cypherpunk Manifesto:
https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt

The Crypto-Anarchist Manifesto:
https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html

Bibliography

Chohan, Usman W., Cryptoanarchism and Cryptocurrencies (November 27, 2017). Available at SSRN: https://ssrn.com/abstract=3079241 or http://dx.doi.org/10.2139/ssrn.3079241

Crypto Anarchy, Cyberstates, and Pirate Utopias, edited by Peter Ludlow, The MIT Press Cambridge, Massachusetts, 2001.

Husain, S.O., Franklin, A. & Roep, D. The political imaginaries of blockchain projects: discerning the expressions of an emerging ecosystem. *Sustain Sci* **15,** 379–394 (2020). https://doi.org/10.1007/s11625-020-00786-x

Markey-Towler, Anarchy, Blockchain and Utopia: A theory of political-socioeconomic stems organised using Blockchain, School of Economics, University of Queensland, 2018. doi: 10.31585/jbba-1-1-(1) 2018.

MacDonald Trent.J., Allen Darcy W.E., Potts Jason, "Blockchains and the Boundaries of Self-Organized Economies: Predictions for the Future of Banking", In: Tasca P., Aste T., Pelizzon L., Perony N. (eds) Banking Beyond Banks and Money. New Economic Windows. Springer, Berlin, 2016.