Culture, decentralized

Cypherpunk influences in western culture

Victor Rudolfsson
Information Security
Høgskolen i Gjøvik
Gjøvik, Norway

I. Introduction

The cypherpunk movement was a seemingly short-lived movement that rose to prominence in the late 80s, and had its golden days during the 90s. It has, however, influenced our culture more than one may think – whether accidentally or not.

Media has experienced a drastic paradigm shift in recent years, what with the internet taking over more and more of its role to bring information out to the general public through means of social media, weblogs, and even personal news papers. Media as we used to know it is no longer based on corporate sponsored news papers or TV channels, and what and who can be defined as the 'press' is becoming more and more diffuse.

That being said, the internet has grown into a media channel where anybody can participate not only as a passive consumer but as an active contributor. This has lead to some controversial issues that came as a result of the ease of publishing information, such as WikiLeaks [1] or OpenLeaks [2], allowing whistle-blowers to publish classified information traditional media otherwise may have chosen not to publish; as well as less controversial services such as social networks.

In recent years, suggestions for virtual currencies relying on cryptographic algorithms and mathematical laws have surfaced as well – BitCoin being a prominent example – and the economy around it is growing [3][4]. This has further lead to more and more legislative proposals to try to control the otherwise uncontrolled medium, which in turn has lead to several suggestions to decentralize the entire internet, one such project called being Project MeshNet [5].

With growing decentralization of economy, press and even the internet itself, central institutions risk having their power redistributed, but how can this affect western culture?

II. Origin of Cypherpunk and Cryptoanarchism

Until around the 70s, encryption was almost only used for military purposes, however, by the end of the decade two publications in particular brought encryption to the public eye – the DES (Data Encryption Standard) and the Diffie-Hellman key exchange. This sparked a discussion about cryptography, which lead to an online group referred to as *cypherpunks*, consisting of people interested in cryptography and the protection of privacy, which by the end of the 80s had started to seem more like a movement than just an online group. Their main source of communication was originally the *cypherpunk mailing list* and subsequently its forks and successors.

The cypherpunks were the origin of *cryptoanarchism*, which was originally described as a type of anarcho-capitalism as they realized it would one day be possible to create a virtual currency to allow for trade and commerce by using cryptographic algorithms. Thus, cryptoanarchism is a more politically focused ideology and a branch of anarchist philosophy that focuses on the use of technology to protect privacy and gain autonomy from governments and in some cases corporate actors in communication, trade and information security. [6]

These core values have had a lot of influence on our western society in recent years, whether intentional or not, in the form of social media and publishing platforms bringing the outreach of traditional media from central institutions to individuals; currency from the control of central authoritative bodies to the laws of math and cryptography; and perhaps even the internet itself from the dependency of service providers to the dependency of connected clients in a way never seen before.

III. Media and Press Decentralization

Social networks such as Twitter and Facebook has allowed individuals to report on events from all over the world, and mobilize faster than ever before. One such event in recent times is the so-called *Arab Spring* in 2011, during which several countries experienced a wave of protests and demonstrations which eventually lead to the fall of several well established regimes, most notably in Egypt, Libya, Tunisia and Yemen. The protests and public uprising making up this event was largely organized by the use of social networks, and may not have been possible without them. During the Arab Spring, 88.1% of surveyed Tunisian citizens and as many as 94.29% of surveyed Egyptian citizens claim they got their information on news and events from social networking sites such as Twitter, and Facebook. [7]

The possibility of allowing any person to broadcast messages to the rest of the world, and for these messages to reach the rest of the world, has allowed ordinary people to act as reporters by reporting on events live by the use of mobile devices.

IV. Economic Decentralization

In 2009 a white-paper submitted under the name *Satoshi Nakamoto*, which is believed to be a pseudonym, proposed an idea for how to create a virtual currency based on mathematical laws and cryptographic algorithms, called BitCoin. BitCoin was later developed into a real currency, and has seen steady growth since its inception, with more and more vendors accepting BitCoin as a method of payment. BitCoin has no central institutions, but relies on a distributed cryptographic block-chain for its integrity and volunteer computers to verify transactions through a process called *mining*. BitCoin's inflation is predictable, as it will grow steadily over the years until it reaches an end point where growth stops – similar to the old monetary system of gold resources: the value of gold will keep dropping as more and more gold is mined and the supply increases, until there is no more gold to mine.

Because BitCoin has no central point, and nobody has heard from the author since the publication of the original white-paper, shutting it down is not a simple task. [8]

V. Connective Decentralization

In 2011, a team that sprung from a project called p2p-dns (*peer-to-peer dynamic name server*) formed to continue their work on a protocol called *cjdns* as a response to recent attempts by the United States attempting to censor content on the internet. To get away from the centralized system of ICANN (*Internet Corporation for Assigned Names and Numbers)* they set out to make this corporation obsolete.

The proposed solution became a protocol called *cjdns*, which aims to solve technical issues with the internet (such as the growing global routing table), management issues (such as different entities attempting to gain control), and security issues by encrypting data end-to-end by default.

The idea of it is that no single point should need to have all information of where a packet should go, and every connected client can participate in routing packets, creating a mesh of connected nodes with no central point. [9]

VI. Conclusion

Whereas the decentralization of several important parts of our culture – economy, press and connectivity – may not be a deliberate move from neither cryptoanarchist nor cypherpunk movements, it has a clear relation to these movements core values, and the impact of which may only have begun to shine through. The growth of social networks has increased rapidly in less than a decade, with more than 14% of the worlds population using Facebook alone. [10]

BitCoin has only just begun to show its potential as a virtual currency, with millions of dollars worth of BitCoins in existence and millions of transactions taking place every single day – yet it has only existed for a few years, and has grown extensively since its inception.

Projet MeshNet, a project utilizing the cjdns protocol which is still only in its early stages, allows anybody to set up their own cjdns node to participate in building an alternative internet, but its potential has yet to be proven in practice.

In times when more and more proposals for control over our media, economy and connectivity are being suggested, perhaps the decentralization of these can lead to a more democratic culture in which individuals can participate actively, and where the ease of which citizens can contribute to their community will help shape the culture of the emerging information age for the better – using technology to let each and every voice be heard, more easily than ever before in human history.

References

[1] Disclosure's Effect: Wikileaks and Transparency, Mark Fenster, University of Florida, 2011, http://www.uiowa.edu/~ilr/issues/ILR_97-3_Fenster.pdf

[2] Wikileaks vs Openleaks: A comparison of approaches, Gilberto Sepulveda, Universiteit Twente, 2011-01-18, http://gilfolio.com/wp-content/uploads/2011/12/Wikileaks-vs-Openleaks_Report.pdf

[3] Total Bitcoins in Circulation, Blockchain.info, https://blockchain.info/charts/total-bitcoins

[4] Cashless Society – A Financial Paradigm Shift Through Social Networking, Manish Parihar, Saraswati Institute of Engineering & Management, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1983157

[5] "The Plan", Project MeshNet, https://wiki.projectmeshnet.org/The_Plan

[6] Cypherrnomicon, Timothy C. May, 1994, http://www.cypherpunks.to/faq/cyphernomicron/chapter16.html#7

[7] Civil Movements: The Impact of Facebook and Twitter, Arab Social Media Report, Dubai School of Government, http://www.dsg.ae/en/ASMR2/Images/report.pdf

[8] Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, http://www.bitcoin.org/bitcoin.pdf

[9] cjdns, Caleb James DeLisle, https://raw.github.com/cjdelisle/cjdns/master/rfcs/Whitepaper.md

[10] Mark Zuckerberg, Chairman & CEO of Facebook, Inc., announcement of passing 1 billion users, 2012-10-04, https://www.facebook.