Beyond Bitcoin Enabling Smart Government Using Blockchain Technology

Svein Ølnes

Beyond Bitcoin
Enabling Smart Government Using Blockchain Technology

Svein Ølnes
Western Norway Research Institute, Sogndal, Norway
sol@vestforsk.no

Abstract. The new technology Bitcoin has got a lot of attention since it was presented in late 2008 and implemented early 2009. However, the main attention has been to the currency and not so much the underlying blockchain technology. This paper argues that we need to look beyond the currency and investigate the potential use of the blockchain technology to enable smarter governments by utilizing the secure, distributed, open, and inexpensive database technology. The technology is discussed in the perspective of an information infrastructure to investigate its full potential. After a literature review of Bitcoin publications, with a special emphasis on eGovernment literature, the paper presents a relevant use case highlighting the innovation potential of the new technology. The literature review shows that Bitcoin is absent from the e-Government literature. The use case presented shows that Bitcoin could be a promising technology for validating many types of persistent documents in public sector.

Keywords: e-Government, bitcoin, blockchain, information infrastructure

1 Introduction

Once in a while technological breakthroughs occur that open up a whole new world of possibilities. Internet itself was a breakthrough like this, and the invention of the web, with its HTTP protocol built on top of the Internet the protocols, likewise opened up a new world of possibilities. To many the breakthrough in trustless commerce and payment made possible with the Bitcoin protocol holds a bit of the same potential as the aforementioned examples [1]. For the first time in history a system has been made that enables secure transactions to be carried out in an unsecure, unreliable environment like the Internet without the need for a trusted third-party. The way this is done is explained in more detail in section two.

Public sector faces a number of challenges, not least in more cost efficient use of ICT and better interoperability between systems, as Codagnone and Wimmer (eds.) states [2]. Dawes et al. looks at information boundaries and the necessity of going from "need to know" to "need to share" and suggests public sector knowledge networks [3]. For higher education, which is the sector where the use case discussed in this paper comes from, the accelerating trend of globalization [4] puts even more pressure on finding solutions that are interoperable on a global scale. Proving the authentication of documents is a general issue for public sector and finding smarter solutions that scale globally and is cost efficient can help both cutting public sector costs and increase the quality of these services.

The Bitcoin blockchain has global reach and can be viewed as an open, distributed, and trustless database on the Internet. Trustless means that it requires no third-party to secure transactions; the trust lies in the software only. Bitcoin can be seen as a system

for proving ownership both to assets and currencies [5]. It was invented by Satoshi Nakamoto [6], presumably a pseudonym for a person or a group of persons. The peer-to-peer system was released as open source software in 2009 and it enables users to transact directly without an intermediary [7].

Currently the Bitcoin blockchain is limited to handle a theoretical maximum of seven transactions pr. second [8] and is therefore not, as yet, ideal for high volume transactions. However, for efficient storing of more persistent objects and assets it is ideal. The low cost of transactions (transaction fees are typically a few cents) combined with a high degree of security makes promises for a cost efficient and secure way of storing assets of various types and in addition achieve a better interoperability due to the open, distributed, and global architecture. This can also comprise public sector assets like certificates, diplomas, licenses and more.

The research objectives of this paper thus is

- to give an overview of the Bitcoin literature in general and in e-Government in particular
- to study the potential for using Bitcoin technology in public sector services

The objectives will be met by first carrying out a thorough literature review related to Bitcoin and then to study the Bitcoin technology in an information infrastructure perspective. Finally a relevant use case from higher education will be explored to shed light on the possible use of this technology in public sector.

Bitcoin is used throughout the paper as a proxy for crypto-based currency systems. Bitcoin is both a distributed infrastructure (the blockchain) and a currency and the paper tries to be consistent in denoting Bitcoin the infrastructure with a capital 'B' and bitcoin the currency with a small case 'b'.

The following section gives a brief explanation of the Bitcoin technology, to the extent necessary for the paper. This is a conceptual paper and the main method of a systematic literature review is described in section three together with a discussion of the use case method. In section four Bitcoin as an information infrastructure and platform for innovation is discussed to investigate Bitcoin's broader potential. A use case relevant for public sector is explored and discussed in section five before, finally, section 6 concludes with open problems and suggestions for further research on the use of this promising technology.

2 What is Bitcoin?

Bitcoin is a virtual currency connected to a distributed ledger (the blockchain) first presented to the Cryptography mailing list by the posting of a white paper [9] from the author named Satoshi Nakamoto. The white paper was titled "Bitcoin – A Peer-to-Peer Electronic Cash System" [6]. The Bitcoin system enables users to transact directly on an open and unsecure network, like the Internet, without the use of an intermediary.

Like most innovations Bitcoin also builds upon earlier innovations. David Chaum introduced blind signatures when creating DigiCash, the first digital cash system [10].

Adam Back's *HashCash* method presented in 1997 [11] and introduced a hash-based proof-of-Work method also used in Bitcoin [7]. Wei Dai's *b-money* [12] took Back's ideas further and suggested a crypto-anarchy system where full anonymity was the central feature. Finally Nick Szabo presented his idea of *Bit gold*, a system that comprised most of the previous mentioned systems in a digital gold system that was very close to the final Bitcoin system [13].

However, the fundamental problem with avoiding double-spending was still unsolved until the advent of Bitcoin. The problem of establishing trust among untrusted parties, like a transaction between two unknown parties on the Net, is generally known as the Byzantine Generals' Problem and was first formulated by Lamport et al. [14]. The problem was related to computer systems' handling of conflicting information from different parts or components. How can the computer, or in Bitcoin's situation the network, decide which message is the correct one when it gets conflicting messages? Bitcoin has solved this in a proof of concept way.

Bitcoin solved the problem in an elegant way by using the afore-mentioned proof-of-work method inspired by HashCash and combined with a consensus based system among the Bitcoin peers [6]. In Bitcoin the users effectively "vote" with their computing power to prevent double-spending attacks [15]. The security relies on the presumption that the cost of compromising the system must outweigh the profit of doing so.

The most interesting feature with Bitcoin seen from an eGovernment perspective thus is the blockchain technology. Although the blockchain marks the really interesting technology it is crucial to understand the deep interlinking between the currency bitcoin and the underlying blockchain technology [7]. One cannot exist without the other (ibid.). Even if the blockchain can hold assets other than the currency bitcoin, the currency is the central component in transferring ownership of assets and it is the incentive for the miners who guarantee the security of the system (ibid.).

Bitcoin relies on two fundamental technologies from cryptography: public key cryptography for making digital signatures [16] and hash functions for validation [5]. A Bitcoin transaction is a digital signature which signs a transaction containing the payers address, the recipients address, and the amount (of bitcoins) transferred [7]. The transaction is propagated to the Bitcoin network, e.g. the nodes comprising all users of the Bitcoin core program, and eventually bundled with other transactions to be included in a block (ibid.). The new block is attached to the blockchain through a mining process where computer power is used to solve a mathematical puzzle, the proof of work (PoW) part [7]. The blocks can also store other information and instructions and this is where the asset component comes in.

Although the virtual currency itself could have a place in public sector use, this paper looks at the potential use provided by the blockchain technology. Bitcoin provides an infrastructure on which new applications and services can be built. The Internet itself represents an important information infrastructure for permissionless innovation both in private and public sector, and the Bitcoin infrastructure holds many of the same promises in its field, as will be elaborated further on in section four.

3 Methodology

The paper is of explorative and conceptual nature and relies on a systematic literature review [17] of Bitcoin-related papers. In addition to the systematic approach a "snowball" method has also been used (ibid.). For the illustration of potential use of Bitcoin technology in public sector a selected use case with special relevance to public sector has been studied.

It is important to emphasize that the conceptual style of the paper is necessary since the use of Bitcoin is almost non-existent in public sector, something the literature study also shows. The only part of Bitcoin paid attention to by public sector is understandably regulatory questions concerning the currency.

For the Bitcoin status in eGovernment literature the newly updated e-Government Research Library[i] (EGRL) v. 11.5, was used as the primary resource. The EGRL library has an extensive overview of e-Government related research currently containing 7,899 of predominantly English-language, peer-reviewed work in the study domains of electronic government and electronic governance [18]. For the broader coverage of Bitcoin-related academic publishing the Thompson Reuters' Web of Science and Google Scholar were chosen. Finally the source "Bitcoin Academic Research" compiled by Brent Scott [19] was categorized into major research disciplines. Scott's compilation using well-known literature resources like JSTOR, Science Direct, Springer Link, SSRN, Taylor & Francis, Google Scholar, Wiley Online Library and many more shows a growing number of Bitcoin-related publications.

Tabell 1. The growth of academic Bitcoin publications [19]

Year	No. of publications
2008	1[1]
2009	0
2010	1
2011	8
2012	21
2013	63
2014	208
2015	325
2008-2015	**627**

The table below shows a categorization of the papers found using different sources. For the three first sources; the EGRL, Google Scholar, and Web of Science, only search phrases related to Bitcoin/blockchain and e-Government is shown. For the Bitcoin Academic Research source the whole catalogue was categorized into the categories technology, economy, and legal and regulatory. The categories were a result of the screening of the papers. The categorization was done based on the title, the summary of the papers, and the journal. In case of ambiguity the complete paper

[1] Satoshi Nakamoto: «Bitcoin – A Peer-to-Peer Electronic Cash System» [6]

was downloaded and examined.

Tabell 2. Categorization of Bitcoin publications from different sources

Category	**EGRL 11.5**	**Google Scholar**	**Web of Science**	**Bitcoin Academic Research**
Search phrases	"bitcoin" "block-chain"	"bitcoin e-Government" "blockchain e-Government"	[same as for Google Scholar]	-
Economy	0	0	0	244
Technology	0	0	0	241
Legal, regulatory	0	0	0	107
Other	0	0	0	35
Irrelevant	-	-	-	-
Total	**0**	**0**	**0**	**627**

Searches for "bitcoin" or "blockchain" in the e-Government literature database EGRL 11.5 did not give any results nor did the searches for "bitcoin e-Government" or "blockchain e-Government" in Google Scholar or Web of Science. In addition to "e-Government" the word "eGovernment" was also included.

The categorization of the Bitcoin Academic Research compilation [19] shows that most of the publications listed fall within the fields of technology and economy with an almost perfect balance between the two research fields. There are also quite a few publications dealing with legal questions like regulation and governance. The category "other" contains work in different research fields, e.g. environmental issues, social science etc.

From the literature search we can conclude that Bitcoin and crypto currency technology is absent from e-Government research.

We have also used a case study approach [20] and studied a relevant use case to shed light on the possibilities for using Bitcoin technology in public sector services. The use case was chosen because of its high relevance for public sector. The use case method is especially useful in situations where the researcher has little or no control over the object to be studied, and for its usefulness in answering "how" and "why" questions [20]). This is the case for Bitcoin in e-Government context where there to date are no obvious use cases to study.

4 Bitcoin as an Information Infrastructure

In order to be a potential valuable technology for use in public sector Bitcoin needs to be more than a payment solution. The technology needs to be a platform capable to foster innovative derivatives. Kazlan et al. [21] define a digital platform as "*a proprietary or open modular layered technological architecture that support efficient development of innovative derivatives*". Bitcoin is published as open source software and is thus an open technological architecture. A number of alternative digital

currencies have been created on the basis of Bitcoin's source code, all with their special features separating them from Bitcoin itself. This shows that Bitcoin is able to support efficient development of innovative derivatives and that Bitcoin as such meets the requirements applied to an open, digital platform.

Information infrastructures (IIs) on the other hand represent another level of complexity by combining social and technical dimensions [22]. Hanseth and Lyytinen (ibid.) define an information infrastructure as "*a shared, open and unbounded, heterogeneous, and evolving socio-technical system consisting of a set of IT capabilities and their user, operations, and design communities*". This definition highlights what they call the emerging properties of IIs. In addition they also point to the structural properties, e.g. organizing principles and control. Examples of IIs are Internet itself, electronic market places, EDI, and wireless service infrastructures to mention a few (ibid.). Hanseth and Lyytinen [22] point to the considerable benefits successfully constructed and implemented IIs hold, as exemplified by Internet, but also at the potential risks involved in designing such systems, again exemplified by the nation-wide e-health system i UK, the ICT part of the National Health Service (NHS). If Bitcoin can be showed to share some of the core properties of an II we can assume that the potential for far-reaching application, including public sector, is high.

IIs distinguish themselves from traditional classes of IT solutions such as IT capabilities, applications, and platforms by being more complex [22]. IIs are thus seen as a more complex unit than platforms. A main difference between an II and a digital platform is the central control of platforms in contrast to the distributed and dynamically negotiated control of IIs (ibid.).

Bitcoin can be seen as an information infrastructure in that it meets the definition. The characteristic properties of an information infrastructure and how these applies to Bitcoin is showed in the table below and discussed in more detail below the table. The table builds on Hanseth and Lyytinen [22], p. 3.

Table 3. Bitcoin as an information infrastructure

Property	**Information infrastruscture (in general)**	**Bitcoin as an II**
Shared	Universally and across multiple IT capabilities	Yes Bitcoin is universally shared (one only need an Internet connection and download/install a wallet to use/take part)
Open	Yes, allowing unlimited connections to user communities and new capabilities	Yes Bitcoin is open for any users and offering an infrastructure for "permissionless innovation".
Heterogenous	Increasingly heterogeneous both technically and socially	To a certain extent. Bitcoin has already generated many new applications and platforms (thousands of altcoins, emerging sidechains, foundation for new platforms like Ethereum[2])
Evolving	Yes, unlimited by time or	Yes, although it is a bit early to say

[2] Ethereum is a derivative of Bitcoin that focuses on smart, programmable contracts. It uses a separate blockchain with its own currency; named ether [23]

	user community	Although a new technology, Bitcoin bears the signs of an unlimited evolvement. The particular Bitcoin system can wither, but the technology will be brought forward by others
Organizing principles	Recursive composition of IT capabilities, platforms and infrastructures over time	Showing signs of recursive composition. Bitcoin itself is fairly new (seven years), but already a recursive composition of IT-capabilities (e.g. different wallets), platforms (e.g. different altcoins), and infrastructures (e.g. Ethereum and Lightning network) have found place [23], [24]
Control	Distributed and dynamically negotiated	Distributed and dynamically negotiated. Bitcoin is a distributed system based on open source software and changes are dynamically negotiated among the user community (e.g. substantial changes need to have a majority of "votes" in order to be accepted)

An II is *shared* across multiple communities in a multitude of ways ([22] and should in principle exhibit unbounded *openness* by including new components in many, including also unexpected, ways. Bitcoin is universally shared by adhering to the protocols of the web (the HTTP protocol) and is released as open source software. Components added to the Bitcoin network range from several types of wallets (e.g. desktop wallets, mobile wallets, hardware wallets, paper wallets), a range of exchange services (e.g. physical ATMs, online exchange services), and mining components. Everybody can run a Bitcoin full client and such be a peer in the network, or on the other hand one can also use a light-weight version of Bitcoin; typically a mobile wallet. The mining operation of the Bitcoin system is also open although at present it requires specialized hardware in order to gain more than the cost of equipment.

Because of the openness an II should also be *heterogeneous* implying that social and technical diversity should increase during the lifetime (ibid.). Bitcoin is a fairly new technology, but already we see great social and technical diversity with applications and platforms like altcoins (more than 3,300 to date[3]), smart contracts [23], sidechains for reducing the load on the main Bitcoin blockchain [25], micro payments systems built on top of Bitcoin [24], coloured coins to represent different types of assets [26], Bitcoin blockchain for secure domain name handling [27] and many more digital implementations as well as physical constructions like ATMs.

Also because of the openness IIs should *evolve* constantly (ibid.). Again Bitcoin, including the blockchain technology, is not mature. However, already in the first seven years the technology has shown a remarkable development from being used by a handful of persons the first year to today's millions of users (nodes) and links [28], high investment rate indicating lots of start-ups, and a continuous expansion also in terms of diversity of components and services added to the technology.

When looking at the structural properties the *organizing principle* of an II should be a recursive composition of IT capabilities, platforms and infrastructure over time [29]. The bootstrapping process by experimenting is also evident in the Bitcoin

[3] http://www.cryptocoincharts.info/coins/info

development first designed as a payment method and later having evolved into a range of possible uses. The bootstrapping process for Bitcoin and other crypto currencies is also special since it is both a technology and a financial structure. The system is especially vulnerable in the bootstrapping process due to the proof of work method. It will be relatively easy to compromise such a system in the beginning because of the low requirements for PoW resources. This will also increase the "first mover advantage" because over time the infrastructure will grow more and more robust while competing systems will have trouble bootstrapping.

Finally the structural property of *control* typical for an II is distributed and dynamically negotiated one [30]. Bitcoin is clearly a distributed technology with no central control. The main purpose of its design was to avoid central control in the form of a trusted third-party. It was presented as a peer-to-peer technology from the beginning [6]. The recent debate over the block size [31] also shows that no party is in control of changes to be made and that these changes must be negotiated dynamically: miners have their say, full node clients have their say, and core developers also have their say, but none of the groups can dictate the terms. This has been, and is, a very heated debate and the community has not reached a conclusion yet [32].

The use case presented in the next section will be discussed in light of digital platforms and information infrastructures.

5 Use Case: Academic Certificates Stored on the Blockchain

Andreas Antonopoulos is one of the most experienced Bitcoin technologists and the author of "Mastering Bitcoin" [7]. In addition to serving on the advisory board for many start-up companies in Bitcoin technology he is also a Teaching Fellow at the University of Nicosia where he teaches the online courses in digital currencies. After finishing the first teachings of the MOOC-based[4] course "Introduction to Digital Currencies" he decided to store the academic certificates for all the students who successfully completed the course on the Bitcoin blockchain [33]. After all, one of the great promises of the blockchain technology is that it can serve as a decentralised, permanent, and utterly secure store for all types of assets, not just as a currency. That is what makes it interesting also for public sector use.

The following basic requirements were set up before the project of storing the academic certificates on the blockchain started: a) the process should involve no other services or products other than the Bitcoin blockchain, b) the process should allow someone to authenticate a University of Nicosia certificate without having to contact the University of Nicosia, and c) The process should allow someone to complete the process even if the University of Nicosia, or more likely their website, no longer existed. The University of Nicosia is a private university, but this use case is just as relevant for a public university.

The process of storing the academic certificates on the blockchain followed these steps [33]:

[4] MOOC = Massive Open Online Courses

Hash of the individual certificates. A hash of a certificate is at the core of the process. A hash function is a one-way function that takes any arbitrary data as input and produces a string with a fixed number of characters [16]. In Bitcoin the SHA-256 hash function is used [7].

Index put on the blockchain. Instead of storing each individual certificate on the blockchain an index document containing the hashes of all the certificates were created and the hash value of the index document stored on the blockchain. The hash of the index document was entered to the blockchain in an unspendable Bitcoin transaction to serve as the permanent record underpinning the whole approach.

Timing and instructions. The certificates had to be self-verifying the timing of entering of the hashed index on the blockchaincritical.

Public access. The index document containing the hashes of all the individual certificates is published on the University of Nicosia homepage. But if this was all, there would be no use for the blockchain. For the process to be truly decentralised people should be able to find a copy of the index document anywhere on the web and compare it to the index document on the blockchain.

The verification process is carried out in two steps; one for verifying the index document and the second for verifying the particular certificate:

Verifying the index document. Ensure that a valid index document from the University of Nicosia is used. The hash of the index document should be the same as the hash stored on the blockchain, in the specified timeframe.

Verify the certificate. Once the index document has been verified, a SHA-256 hash of the certificate (in pdf) should be compared to the hash of the same certificate listed in the index document. If the hash values are similar, the certificate is authentic. Of course, the comparison of the hash values only guarantees the authenticity of the certificate, not that the person who sent the certificate is the same as the person on the certificate. That has to be validated in other ways.

The use case above has shown one possible use of the Bitcoin blockchain technology for public sector. All organizations issuing certificates, licenses etc. could benefit from the new technology, as this use case shows. The use case from the University of Nicosia has pointed to a couple of challenges that should be investigated more in depth in order to arrive at a best practice for storing certificates and licenses on the blockchain.

The Bitcoin technology fits the definition of a digital platform and the characteristics of an information infrastructure can also be found in the technology, as shown in table 3. Its dispersed and distributed “ownership” is in line with the central attribute of an II. *Installed base* is another key element in an information infrastructure and denotes technical and non-technical elements illustrating the network effects determining the development of the infrastructure [22]. The installed base in this case is the organisational, economic, and legal factors governing today’s public service II. The legal factors are of special importance, as is also discussed in many of the publications listed in section three. However, the legal and regulatory

factors discussed in these papers are mostly about regulating the currency and the payment system. The use case described above, and similar uses of Bitcoin, escapes these worries since the payment part is just a necessary side effect and not the goal itself. That is the case with all use cases belonging to so-called "smart contracts" use of Bitcoin. The currency is used only as a token in these cases.

An information infrastructure without direct Government control might seem scary for public sector. When considering Bitcoin as an interesting technology in e-Government we need to review history and be reminded of the "battle" between global network standards in the end of the 1980s, beginning of 1990s. Governments had the choice between the controlled OSI protocol and the Internet protocol, and most of them chose the OSI protocol. USA's Government OSI Profile – GOSIP – became the standard for many other nations' OSI profiles, e.g. NOSIP – Norwegian OSI Profile [34]. Internet's rise in popularity made it a de facto standard that soon overrun the OSI protocol, not least because the OSI standards struggled to deliver working and interoperable services (ibid.). Internet became the national and international standard for global communication not because of national priorities, but despite them. This is something to bear in mind when considering a technology that uses the same distributed model that Internet itself.

6 Conclusions and Further Research

This paper has shown that the topic Bitcoin technology is absent from e-Government literature. The major part of academic publishing on Bitcoin has been in the fields of technology, economy, and regulation. Of course, one explanation why Bitcoin and blockchain is absent from the e-Government literature could be that the technology does not have any potential benefit for public sector, but that is hardly likely. At least researchers should provide arguments for why this could be the case.

Bitcoin meets most of the core requirements for an information infrastructure and is thus well positioned to have a broad impact on future digital innovation. The use case detailed and analyzed in the chapter above shows that Bitcoin also has a great potential for use in public sector. Storing certificates on the block-chain is a cost-effective way of storing and securing vital information. The use case shows that this is possible for certificates, but also that this could be a promising technology for all types of permanent, or relatively permanent, public documents. Other examples could include contracts of different types (e.g. procurement contracts), licenses (e.g. driving licenses), and many more given its information infrastructure capabilities.

Having a great potential is not the same as having a great success. There are quite a few examples of technologies with great potential nevertheless failing to be embraced and included in the technologies used for everyday service provision.

However, given the promising benefits the Bitcoin technology holds it is important that also researchers in the e-Government field starts to investigate it. There are a lot of questions that need to be answered by doing more research. Among the many research questions are how can the Bitcoin blockchain technology help innovate the development of digital services from public sector? How should the currency and the blockchain part of the Bitcoin protocol be handled by public agencies? Should public sector use a separate sidechain and if so, what would be the major threats to such a

strategy? What are the important factors determining the adoption of Bitcoin technology in public sector? And with regard to Bitcoin as an information infrastructure: what is the crucial installed base determining whether Bitcoin will succeed or not in public sector?

These questions are not that different from the questions of public sector's use of Internet and the web in the beginning of the 1990s. Perhaps going back 25 years and looking at how these questions were answered can give us an idea of how public sector should approach the Bitcoin technology.

Acknowledgement
Thanks to Satoshi Nakamoto for giving us this radical technology to build on.

References

[1] M. Andreessen, "Why Bitcoin Matters." New York Times, 21-Jan-2014.
[2] C. Codagnone and M. A. Wimmer, *Roadmapping eGovernment Research: Visions and Measurestowards Innovative Governments in 2020.* Guerinoni Marco, 2007.
[3] S. S. Dawes, A. M. Cresswell, and T. A. Pardo, "From 'need to know' to 'need to share': Tangled problems, information boundaries, and the building of public sector knowledge networks," *Public Administration Review*, vol. 69, no. 3, pp. 392–402, 2009.
[4] P. G. Altbach, L. Reisberg, and L. E. Rumbley, *Trends in global higher education: Tracking an academic revolution*. UNESCO Pub.; Sense, 2009.
[5] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, Technology, and Governance," *The Journal of Economic Perspectives*, vol. 29, no. 2, pp. 213–238, 2015.
[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Consulted*, vol. 1, no. 2012, p. 28, 2008.
[7] A. M. Antonopoulos, *Mastering Bitcoin - Unlocking Digital Cryptocurrencies*, 1st ed. San Francisco, 2014.
[8] A. Zohar, "Bitcoin: under the hood," *Communications of the ACM*, vol. 58, no. 9, pp. 104–113, 2015.
[9] H. Karlstrøm, "Do libertarians dream of electric coins? The material embeddedness of Bitcoin," *Distinktion: Scandinavian Journal of Social Theory*, vol. 15, no. 1, pp. 23–36, 2014.
[10] D. Chaum, "Blind signatures for untraceable payments," in *Advances in cryptology*, 1983, pp. 199–203.
[11] A. Back, "Hash cash: A partial hash collision based postage scheme," *URL http://www. hashcash. org*, 2001.
[12] W. Dai, "B-money," *Consulted*, vol. 1, 1998.
[13] N. Szabo, *Bit gold*. Website/Blog, 2008.
[14] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382–401, 1982.
[15] A. Gervais, V. Capkun, S. Capkun, and G. O. Karame, "Is Bitcoin a decentralized currency?," 2014.
[16] B. Schneier, "Applied Cryptography–Protocols, Algorithms, and...," 1994.
[17] R. B. Briner and D. Denyer, "Systematic review and evidence synthesis as a practice and scholarship tool," *Handbook of evidence-based management: Companies, classrooms and research*, pp. 112–129, 2012.

[18] H. J. Scholl, “eGovernment Reference Library (EGRL) version 10.5.” University of Washington, 2015.
[19] B. Scott, “Bitcoin Academic Research,” *The Heretic’s Guide to Global Finance: Hacking the Future of Money*, 30-Dec-2014. .
[20] R. K. Yin, *Case Study Research: Design and Methods*. SAGE Publications, 2013.
[21] E. Kazan, C.-W. Tan, and E. T. Lim, “Towards a Framework of Digital Platform Disruption: A Comparative Study of Centralized & Decentralized Digital Payment Providers,” 2014.
[22] O. Hanseth and K. Lyytinen, “Design theory for dynamic complexity in information infrastructures: the case of building internet,” *Journal of Information Technology*, vol. 25, no. 1, pp. 1–19, 2010.
[23] D. G. WOOD, *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER*. Ethereum, 2014.
[24] J. Poon and T. Dryja, “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments,” Technical Report (draft). https://lightning. network, 2015.
[25] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, “Enabling blockchain innovations with pegged sidechains,” *URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains*, 2014.
[26] M. Rosenfeld, “Overview of colored coins,” *White paper, bitcoil. co. il*, 2012.
[27] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, “Blockstack: Design and Implementation of a Global Naming System with Blockchains.”
[28] D. Kondor, M. Pósfai, I. Csabai, and G. Vattay, “Do the rich get richer? An empirical analysis of the Bitcoin transaction network,” *PloS one*, vol. 9, no. 2, p. e86197, 2014.
[29] P. N. Edwards, S. J. Jackson, G. C. Bowker, and C. P. Knobel, “Report of a Workshop on ‘History & Theory of Infrastructure: Lessons for New Scientific Cyberinfrastructures,’” *Understanding Infrastructure: Dynamics, Tensions, and Designs*, 2007.
[30] P. Weil and M. Broadbent, “Leveraging the new Infrastructure,” *Harvard Business School Press. Boston*, 1998.
[31] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, and E. Gün, “On Scaling Decentralized Blockchains,” in *Proc. 3rd Workshop on Bitcoin and Blockchain Research*, 2016.
[32] M. Pilkington, “Blockchain Technology: Principles and Applications,” *Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar*, 2016.
[33] University of Nicosia, “Academic Certificates on the Blockchain,” *MSc in Digital Currency - University of Nicosia*, 2014. [Online]. Available: http://digitalcurrency.unic.ac.cy/certificates. [Accessed: 01-Jul-2015].
[34] B. Ness, *Tilkoplet - En fortelling om Internett og Forskningsnettet i Norge*. Fagbokforlaget, 2013.