Blockchain Technology as a Support Infrastructure in e-Government

Svein Ølnes[1] and Arild Jansen[2]
[1]Western Norway Research Institute, Sogndal, Norway
sol@vestforsk.no
[2]University of Oslo, Oslo, Norway
arildj@jus.uio.no

Abstract. The blockchain technology, including Bitcoin and other crypto currencies, has been adopted in many application areas during recent years. However, the main attention has been on the currency and not so much on the underlying blockchain technology, including peer-to-peer networking, security and consensus mechanisms. This paper argues that we need to look beyond the currency applications and investigate the potential use of the blockchain technology in governmental tasks such as digital ID management and secure document handling. The paper discusses the use of blockchain technology as a platform for various applications in e-Government and furthermore as an emerging support infrastructure by showing that blockchain technology demonstrates a potential for authenticating many types of persistent documents.

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

1 Introduction

Bitcoin and the underlying blockchain technology have met with significant acceptance in recent years. Since its inception less than ten years ago, primarily as a crypto currency, the technology has been developed as a platform for various applications in different areas, not only in the banking and financial sector. We find applications in other areas where secure transactions have to be carried out in an otherwise unsecure, unreliable environment like the Internet, even without the need for a trusted third-party [1,4]. Bitcoin, including peer-to-peer networking, blockchain and consensus mechanisms provide secure identification and authentication in various types of distributed computing environments.

Some of the most important features of the open blockchain technology are its global nature and reach, its built-in transparency and its independence of third party trust. These features are not of equal importance for all governments but will be more important in countries vulnerable to corruption and lack of trust in general than in countries that enjoy a high degree of trust from its citizens and businesses. However, also these countries can benefit from the global reach and transparency that the open blockchain technology offers.

Although blockchain technology has grown remarkably as a support for many innovations, it is still a somewhat immature technology. The blockchain technology at the present time seems primarily suitable for digital ID management and secure record-keeping and document-handling, which of course are core governmental activities. A blockchain contains a secure, verifiable record of every single transaction ever made [2], whether it is a financial transaction or a transaction involving a governmental procedure (e.g. recording and timestamping a public document). This gives the technology a potential for beneficially changing secure document management in the public sector.

Secure document-handling functions, including digital signatures, certificates etc., are still an area having many different systems and practical arrangements and often creating a lot of confusion for non-specialist users.

The blockchain technology offers a high level of security; the administration of a blockchain based document management may become simpler, and not least, it will be open and more transparent.

The specific aim of this paper is to discuss in what ways and the extent to which the Bitcoin blockchain technology can be regarded as a general platform and possible service infrastructure. Thus the research objectives of our paper are:

To understand the Bitcoin/blockchain technology as
(1) an emerging platform
(2) potentially a support infrastructure for improving the digitalization in public sector

A brief clarification of our terminology is needed. We use "Bitcoin/blockchain technology" throughout the paper to mean the blockchain network and database that are underlying Bitcoin, including the peer-to-peer networking, consensus rules and security mechanisms (even though this term has been criticized by e.g. Valkenburgh [3]. Otherwise, we will explicitly name the specific platform or application in question. In addition, Bitcoin with a capital 'B' is used to denote the system while bitcoin with a small 'b' is used to denote the currency. Furthermore, our paper mainly discusses open blockchains [networks], because closed systems are never able to build an infrastructure.

Method description

Our research approach is exploratory, analyzing the diffusion of blockchain technology in an information-infrastructure perspective. The conceptual style of the paper is most appropriate since the use of blockchain technology is almost non-existent in e-Government, as recent publications show [4]. The regulatory side of crypto currencies is important for governments, but it falls outside the scope of this article.

Our selection of literature is based on the snow-ball method [5], starting with seminal research papers on the subject, then including their referenced papers. We have also searched the extensive e-Government Research Library (EGRL) v. 12.0. However, although the EGRL 12.0 contains a huge collection of peer-reviewed papers within the e-Government field, almost no references can be found to Bitcoin and/or blockchain technology. This was also confirmed in a literature study from 2016 [4]. In the added publications in EGRL since v. 11.5 from 2016 a paper on virtual currency regulation can be found [6] searching for "bitcoin" or "blockchain". The latter paper, however, is not relevant to our discussion.

Structure of the paper

The rest of the paper is organized as follows. Chapter 2 provides a description of the technological foundation, focusing on the Bitcoin and the blockchain technology and some current applications. Chapter 3 analyzes this technology in an information infrastructure perspective. In Chapter 4, we discuss some potentially interesting applications of the technology within the application area of digital ID management, including authentication, and the last chapter concludes our findings by addressing future research.

2 Bitcoin and Blockchain Technology

The virtual currency bitcoin is associated with a distributed ledger technology called the blockchain. It was first presented to a cryptography mailing list [7] by the posting of a white paper titled "Bitcoin – A Peer-to-Peer Electronic Cash System" in late 2008 by an author named Satoshi Nakamoto [8], presumably a pseudonym. The Bitcoin system enables users to transact directly in an open and unsecure network, like the Internet, without the use of an intermediary. This peer-to-peer system was released as open source software and launched in 2009 [7]. It has been running continuously since then and has grown to facilitate several hundred thousand transactions per day.

Bitcoin builds on research in cryptography including earlier attempts to create virtual currencies ([10], [11], [12], and [13]). The core principles of Bitcoin are (1) the peer-to-peer architecture, (2) the novel use of blockchain as storage, including time stamping and validation of transactions, and (3) the consensus mechanisms framing the rules and the security model [3]. The blockchain itself is a distributed database that maintains a continuously growing list of ordered records called *blocks*, containing *transactions*. A transaction can hold different types of data. Each block contains a timestamp and a cryptographic link to the previous block [9]. In Bitcoin, the individual bitcoins are also linked together through the transactions (ibid.).

Currently the Bitcoin blockchain is limited to handling a theoretical maximum of seven transactions per second [8] and is therefore not ideal for high volume transactions. However, for efficient storing of more persistent objects and assets (e.g. certificates, licenses etc.) it is ideal. These types of objects do not change ownership so frequently that the relatively slow transaction speed of Bitcoin is challenged. The relatively low cost of transactions, combined with a high degree of security, promise cost-efficient and secure storage of various types of assets, in addition to interoperability due to its open, distributed,

and global architecture. This can also consolidate assets like certificates, diplomas, licenses etc. The public sector can benefit from a readily available platform and possibly avoid costly investments.

Bitcoin solved the former problem of avoiding double-spending (spending a single digital token twice) by using a proof-of-work (PoW) method inspired by HashCash [11] and Reusable Proof of Work (RPOW) [15] combined with a consensus-based system among the Bitcoin peers [8]. The PoW-based security model relies on the presumption that the cost of compromising the system must outweigh the profit from doing so. The PoW in Bitcoin is primarily to find a hash value based on the combination of the hash value of the previous block, a "nonce" and the hash of the new block [9]. Hash functions are used for authentication of documents and are also crucial in verifying and validating digital signatures [16].

Although this paper focuses on the blockchain technology per se, it is important to understand how the bitcoin currency and the underlying blockchain technology is tightly interwoven [9]. An open, permissionless blockchain cannot exist without incentives or recompensing mechanisms like Bitcoin (ibid.). Even if the blockchain can contain information other than the bitcoin currency transactions, the currency is a crucial incentive to secure the transfer of ownership of information and assets. The possibility to earn new bitcoins is what keeps miners spending resources (mainly hardware and electricity) on finding the specific hash value and thereby securing the transactions (ibid.). The massive amounts of resources spent on computing hash values make Bitcoin by far the most secure blockchain system in operation today [17].

There is a common misconception that blockchain technology itself comes with a built-in security [3]. Instead, the opposite is true; the security mechanism needs to be specified. There is a fundamental difference between an open blockchain and a closed (private) blockchain [3]. *Open* blockchains, like e.g. Bitcoin and Ethereum, are permissionless systems in which everyone can join and even develop additional solutions, and therefore they need a security model to secure the transactions and, furthermore, to integrate a consensus mechanism. The only model operating at scale today is the PoW model. *Closed* blockchains, on the other hand, must rely on traditional security mechanisms in order to prevent unwanted access and modification to the blockchain.

At a technical level, Bitcoin relies on two fundamental cryptographical functions: public key cryptography for making digital signatures [18] and hash functions for validation of signatures and transactions [1]. A Bitcoin transaction is a digital signature which signs a transaction containing the payer's address, the recipient's address, and the amount of bitcoins transferred [9]. 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 [9]. The miner who first finds the right answer to the puzzle gets a reward in newly minted bitcoins. Miners' contribution in the Bitcoin system together with the control mechanisms of full node clients render it possible to eliminate the use of a third-party for approval [8].

Bitcoin was the first implementation of a virtual currency system. During subsequent years, numerous copies have been made, resulting in new virtual currencies called *altcoins*; at present there are hundreds of them (see coinmarketcap.com). These altcoins can also be seen as alternative platforms for digital currency solutions and real-life and real-time testbeds for new features. Among these are Ethereum, focusing on smart contracts [19], Monero, Dash and Zcash, all of which provide more privacy than Bitcoin [20].

An important part of blockchain development is its governance. In Bitcoin, no group of stakeholders (e.g. miners, full node clients, core developers) is in charge, and consensus between the different groups has to be reached. Changes to the protocol are proposed through BIPs (Bitcoin Improvement Proposals) and are then voted on by miners. Full node clients "vote" by downloading upgraded versions of the reference client, or choosing not to download [21]. However, the recent scaling debate concerning whether to raise the size of blocks to achieve better throughput and ease the pressure of unconfirmed transactions piling up has raised concerns and caused many people to describe the debate as a governance crisis [21]. Bitcoin does not have any way of managing conflicts and that can lead to paralyzing deadlocks, which seems to be the situation now (ibid.). The governance of blockchain technologies is important if the technology also is to be used as a platform for public digital services.

Almost all altcoins derive from Bitcoin and share the fundamental design principles. They distinguish themselves from Bitcoin in different ways, e.g. monetary policy, capacity, hashing methods etc. Altcoins are incompatible with Bitcoin, and when a crypto currency performs a hard fork (a change in

protocol that is not backward compatible), there is a risk that a new altcoin will be the result, if the participants do not agree unanimously on the change. An example of this is the Ethereum platform that split in two (Ethereum and Ethereum Classic) after a controversial hard fork in 2016.

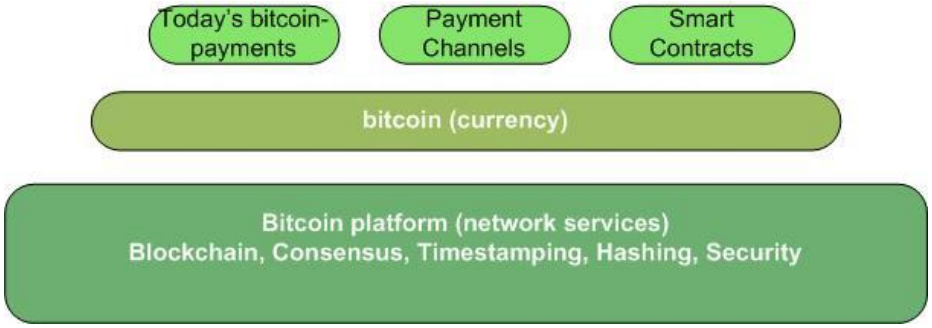

Fig. 1. Bitcoin's layered architecture

3 Blockchain in an Infrastructure Perspective

An ICT infrastructure is usually regarded as the collection of hardware and software components, including networks that are required to enable communication and interoperations between ICT systems. Thus, they form a different "unit" of design when compared with traditional classes of IT solutions. Hanseth and Lyytinen (2011) define these design classes in their order of increasing complexity as: (1) IT capabilities, (2) applications, (3) platforms, and (4) information infrastructures (IIs).

We see that Bitcoin (and other virtual currencies based on blockchain technology) clearly fulfills the characteristics of an application, understood as a suite of IT capabilities, being developed to meet a set of specified user needs within a select set of communities. Furthermore, we will argue that the growth of blockchains (including the consensus and security mechanisms) are becoming platforms for many applications, such as securing document handling and other types of digital assets, gradually building a heterogeneous and growing user base. However, one challenge is how to maintain backward compatibility as well as horizontal equivalence across different combinations of capabilities.

Blockchain technology and information infrastructure

ICT infrastructures, as defined above, are primarily understood as technical facilities. However, the advent of the Internet, and more precisely the worldwide web, illustrated a need for a holistic, socio-technical and evolutionary approach when studying such networks of distributed, and thereby interlinked information systems, usually denoted as information infrastructure. Following Hanseth and Lyytinen [22], we understand *Information Infrastructure (II)* 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."* Because of its dispersed and distributed ownership, the lack of centralized control is a fundamental attribute of information infrastructure. Consequently, different actors shape, maintain, and extend information infrastructure "in modular increments, not all at once or globally" [23].

From the outset, Bitcoin was designed as a cryptocurrency and was not intended to comprise a general-purpose platform for public sector use. However, as we have noted above, a number of new applications have been built on the permissionless Bitcoin/blockchain platform (see e.g. figure 1), clearly indicating the potential of this technology to be *shared* across multiple communities in various ways. Furthermore, its developments also demonstrate its *openness and evolving* nature, including a growing number of new applications, as we have illustrated in Chapter 2.

The *control* of an information infrastructure is typically distributed and dynamically negotiated [24]. Blockchain/Bitcoin is clearly a distributed technology as the main purpose of its design has been to avoid central control, e.g. by trusted third parties. It was developed as a peer-to-peer technology from the beginning [8]. The recent debate over the block size [25] shows that no party is in control of the changes to be made and that these changes must be negotiated dynamically: miners have their say, full node clients have their say as well as core developers, but none of the groups can dictate the terms.

This has been, and is currently, a subject of heated debate, and the community has not yet reached a conclusion [26].

The installed base of blockchain technology

Of particular importance in an information infrastructure is its *installed base*, including both technical and non-technical elements. The evolution of IIs are thus path-dependent due to this "living legacy" of existing technical solutions along with organizational, economic and legal elements, interconnected practices and regulations that are often institutionalized in the organization [23]. An adequate understanding of the installed bases is particular important in building IIs in governments (eGovIIs), as an increasing number of information systems are shared in order to provide online government services., and the dynamics related to these systems often require both forward flexibility and backward compatibility.

Hanseth and Lyytinen (op. cit.) emphasize that the understanding of the installed base of an information infrastructure is essential for its governance, not least in order to handle the existing collection of possible legacy systems, which may be barriers for innovations. Currently, the installed base of the blockchain technology is limited, as its applications have short history (less than 10 years). However, we see significant social and technical diversity where new applications and platforms are emerging, e.g. new altcoins, smart contracts [27], sidechains [28]. In comparison, it took more than 20 years for the Internet to gain acceptance.

The limited installed base may both stimulate and inhibit innovations. On the one hand, it may stimulate the development and diffusion of new applications as there are few "technical bindings" such as, for example, legacy systems, and new users will adopt innovative solutions if they are sufficiently attractive or meet specific needs. The growth of cryptocurrency and various electronic cash systems clearly illustrates this. On the other hand, the lack of bonds to an existing installed base – for example, users of existing applications in relevant areas (such as payment systems, secure document handling and asset management etc.) – may imply that there are few incentives for adoption of applications based on blockchain technology unless they are made more attractive.

However, as we illustrate below, the blockchain technology is evolving beyond its primary application area and already supports a range of secure document and asset management in other areas. We summarize our discussions in Figure 2.

Table 1. The characteristics of different types of infrastructures

Property	Platform	Information infrastructure, e. g. Internet	Blockchain/Bitcoin
Shared	Yes, across involved user communities and across a set of IT capabilities	Universally and across multiple IT capabilities	Potentially shared among those who are involved in building and maintaining this platform
Open	Partially, depends on design choices and managerial policies	Yes, allowing unlimited connections to user communities and new capabilities	Partly yes. Bitcoin is (in principle) open to any users and offers a platform for payment system and secure document/asset handling
Installed base	Growing, but limited to its intended applications and users.	The current Internet applications integrated with its users and use practices, still growing exponentially	The present installed base is limited, which may stimulate innovations but lack the networks effects
Evolving	Yes, limited by architectural choices and functional closure. Linear growth. Path dependent	Yes, unlimited by time or user community. Both linear and nonlinear growth	Yes, although it may be too early to say how. Although it is a new technology, Bitcoin has demonstrated innovative potential.
Control	Centralized	Distributed and dynamically negotiated	Distributed control based on open source software. Changes are dynamically negotiated in user community

Hanseth and Lyytinen [29] distinguish between two types of horizontal IIs: *application and support infrastructure*. We may conceptualize the blockchain technology platform as an emerging support infrastructure, while the Bitcoin and other digital currencies are part of the application layer. By so doing, we do not impose any restriction on how these technologies may evolve, as we do not yet know how new applications, such as secure document handling, smart contracts, digital ID management etc. will be realized on a growing support infrastructure.

Blockchain technology and the Internet – similarities and differences

The structure and development trajectory of the blockchain technology has been compared to that of the Internet [3]. Although such a comparison may result in misleading associations, we believe there are some lessons to be learned from the history of building the Internet.

The kernel of Internet architecture is essentially the TCP/IP protocol suite, built in a layered and modular way. TCP/IP offers a completely distributed, packet-switched network in that it requires no central control when in operation; new nodes may be added or removed in a dynamic way. Internet (IP) packets may be transmitted over any type of physical medium and TCP/IP supports all types of applications. Furthermore, the Internet is transparent and neutral to any type of information being sent across the network (as unfiltered data). As important is its basic characteristic; being open, global and borderless with no censorship. Thus, based on the end-to-end-principle (see e.g. [30]), the Internet may be considered an "unintelligent" network, meaning that there is minimum functionality inside the network, making it efficient, flexible and dynamic.

Similarly, the blockchain platform, including Bitcoin is a dumb transaction-processing network because it pushes all of the intelligence to the edges, thus being able to support various smart devices. It does not offer a range of financial services and products, and it does not have automation and various features built in, thus making the interfaces much simpler, and thereby simpler to support innovations. analogous to Internet [31] The basic properties of the blockchain technology includes consensus rules, peer-to-peer mechanism, security functions such as cryptography and hash functions etc., which are not part of the blockchain database but have to implemented in the hardware/ software controlling and verifying the blockchain.

We do not believe it is fruitful to (strictly) compare the architecture of the Internet with blockchain technology. However, in the figure below we illustrate the analogous structure of these two architectures.

Internet		**Blockchain technology**
Applications		Applications
HTTP/HTML/…		Bitcoin/other currency
TCP/IP		Consensus rules, peer-to-peer, security
Physical and logical link		Distributed blockchain database

Fig. 2. The layered structure of Internet and the Blockchain

Infrastructure growth through bootstrapping

Hanseth and Lyytinen [22] have outlined a strategy for a set of design principles and rules to guide the design so that a set of system features is selected to meet chosen design goals. They exemplify the bootstrap problem (to come up with solutions early on that persuade users to adopt while the user community is non-existent or small): How can ICT solutions in an information infrastructure get a value? We clearly understand that IIs need to meet early users' needs directly in order to fulfill their mission. They thus outlined the following design strategy: i) design initially for usefulness, ii) draw upon existing installed base, iii) expand installed base by persuasive tactics. IIs are often bootstrapped, by experimenting and thereby enrolling new communities, as e.g. Berners-Lee who designed the first WWW services to meet information-sharing needs among high energy physicists, however expanding to a growing, worldwide community [23].

Thus, we believe that the bootstrapping approach is useful to foster the growth of Bitcoin/Blockchain. Although this technology is not yet mature, the technology has shown a significant development from being used by a handful of persons the first year to today's millions of users (nodes) and links [32], significant investment rate indicating lots of start-ups, and expansion in terms of diversity of components and services added to the technology [33] (e.g. different wallets) and platforms (e.g. Ethereum and Lightning network) have found place [34], [35]. In particular, we believe that successful applications in public sector will stimulate such developments.

4 Blockchain Technology in e-Government

Blockchain and innovations

Our research question is "To understand Bitcoin and the underlying blockchain network(s) as (1) an emerging platform and (2) potentially as a support infrastructure". One way to study this is to investigate its generative capacity.

According to Zittrain [36], generativity is a function of a technology's capacity for leverage across a range of tasks, adaptability to a range of different tasks, ease of mastery and accessibility. Generativity denotes a technology's overall capacity to produce unprompted change driven by large, varied and uncoordinated audiences.

Leverage describes the extent to which objects enable valuable accomplishments that otherwise would be either impossible or not worth the effort to achieve. The Bitcoin/blockchain does offer a platform for secure and transparent payment and other financial operations in hostile environments, with no adequate technical or institutional infrastructure in place. For many countries where corruption often appears as a threat to ordinary ways of doing business, not least with the Government, tamper-evident and tamper-resistant ICT systems can provide significant benefits. For example, the Government of Honduras recently started collaborating with the blockchain company Factom (ibid.) aiming to use this technology for storing land title deeds and thereby rendering corruption much more difficult [37].

Adaptability refers to both the breadth of a technology's use without change and the readiness with which it might be modified to broaden its range of uses. As an illustration of blockchain potential, the UK's Government Office for Science [38] have proposed several use cases for blockchain technology that point to using the technology for (1) protecting critical infrastructure, (2) novel payment systems for work and pensions, (3) strengthening international aid systems, (4) document authentication and smart contracts, and (5) handling European VAT. Of these suggested application areas, we think authentication of documents (CVs and other certificates, licenses, intellectual properties and patents, wills etc.) is the most interesting in terms of short–term realization. Thus, using blockchain technology for land title registry is an interesting use case for the public sector, highlighting the use of blockchain technology for secure storage of authentic documents as part of the effort to innovate e-Government solutions. The Swedish Lantmäteriet, responsible for land title and estate registries, collaborates with business partners to investigate the possibilities of using blockchain technology to innovate their ICT solutions [39].

Ease of Mastery A technology's ease of mastery reflects how easy it is for broad audiences both to adopt and to adapt it. Academic certificates have already been stored on the Bitcoin blockchain. The University of Nicosia was probably the first institution to do this with their course "Introduction to Digital Currencies" [4]. The individual certificates from this course were first hashed to produce a fingerprint of the document. The hashes of all certificates from the course were then gathered in one document, which was again hashed, and the resulting fingerprint was stored on the Bitcoin blockchain (ibid.). The MIT Media Lab took this proof of concept further and developed an open source solution called *Blockcert* [40]. The *Blockcert* system is a complete system for storing, verifying and also revoking academic certificates using the Bitcoin blockchain [41]. The overarching idea is that the students should own their own records; this can be achieved by using the technology of open blockchains

Accessibility. The more readily people are able to use and control a technology, along with the information that might be required to master it, the more accessible the technology is. The above examples also show that the blockchain technology is becoming more easy to use. The open and global nature of public blockchains means that the technology is available and accessible to all people, and the only requirement is an Internet or mobile network connection. However, usability has not been given high priority thus far, and the crucial management of keys shares much of the same challenges as similar management from other domains [42].

5 Conclusions and Further Research

This paper has argued that Bitcoin and the underlying blockchain technology is an emerging platform for further innovation not just in financial systems but also in the public sector. The technology

seems to be evolving into a support infrastructure for secure document handling and is thus positioned to have a significant impact on future digital innovations, including in the public sector.

We therefore argue that ICT systems based on blockchain technology, implying decentralized management and control, offer more robust and flexible solutions that cannot be corrupted. However, lessons learned from earlier efforts to introduce new technology underscore the importance of following a realistic, systematic approach. As a first step, we have provided examples of applications areas where the solutions are technically rather uncomplicated, and where there are few organizational or institutional barriers. However, given the promising benefits that blockchain technology holds, it is also important that researchers in the field of e-Government begin discussing important questions: Are governmental agencies ready to investigate the potential of blockchain technology, and what are the main barriers? What are the important factors determining whether to adopt Bitcoin technology in the public sector?

References

[1] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, Technology, and Governance," *J. Econ. Perspect.*, vol. 29, no. 2, pp. 213–238, 2015.

[2] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Appl. Innov.*, vol. 2, pp. 6–10, 2016.

[3] P. van Valkenburgh, "Open Matters - Why Permissionless Blockchains are Essential to the Future of the Internet," Coin Center, Dec. 2016.

[4] S. Ølnes, "Beyond Bitcoin Enabling Smart Government Using Blockchain Technology," in *International Conference on Electronic Government and the Information Systems Perspective*, 2016, pp. 253–264.

[5] R. B. Briner and D. Denyer, "Systematic review and evidence synthesis as a practice and scholarship tool," *Handb. Evid.-Based Manag. Co. Classr. Res.*, pp. 112–129, 2012.

[6] C. G. Manrique and G. Manrique, "The Evolution of Virtual Currencies: Analyzing the Case of Bitcoin," *Inf. Commun. Technol. Public Adm. Innov. Dev. Ctries.*, vol. 195, p. 213, 2015.

[7] H. Karlstrøm, "Do libertarians dream of electric coins? The material embeddedness of Bitcoin," *Distinktion Scand. J. Soc. Theory*, vol. 15, no. 1, pp. 23–36, 2014.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Consulted*, vol. 1, no. 2012, p. 28, 2008.

[9] A. M. Antonopoulos, *Mastering Bitcoin - Unlocking Digital Cryptocurrencies*, 1st ed. San Francisco, 2014.

[10] D. Chaum, "Blind signatures for untraceable payments," in *Advances in cryptology*, 1983, pp. 199–203.

[11] A. Back, *Hashcash - A Senial of Service Counter-Measure*. 2002.

[12] W. Dai, "B-money," *Consulted*, vol. 1, 1998.

[13] N. Szabo, *Bit gold*. Website/Blog, 2008.

[14] A. Zohar, "Bitcoin: under the hood," *Commun. ACM*, vol. 58, no. 9, pp. 104–113, 2015.

[15] H. Finney, *RPOW: Reusable Proofs of Work*. Cypherpunks, 2004.

[16] Wikipedia, "Hash function," *Wikipedia*. 18-Jan-2017.

[17] Let's Talk Bitcoin, *Proof of Work and the Monument of Immutability*, vol. LTB, 310 vols. 2016.

[18] B. Schneier, "Applied Cryptography–Protocols, Algorithms, and...," 1994.

[19] V. Buterin, "Ethereum White Paper: A next-generation smart contract and decentralized application platform," *Ethereum White Pap.*, 2014.

[20] S. Noether, A. Mackenzie, and others, "Ring Confidential Transactions," *Ledger*, vol. 1, pp. 1–18, 2016.

[21] P. De Filippi, "Blockchain-based Crowdfunding: what impact on artistic production and art consumption?," *Obs. Itaú Cult.*, no. 19, 2015.

[22] O. Hanseth and K. Lyytinen, "Design theory for dynamic complexity in information infrastructures: the case of building internet," *J. Inf. Technol.*, vol. 25, no. 1, pp. 1–19, 2010.

[23] S. L. Star and K. Ruhleder, "Steps toward an ecology of infrastructure: Design and access for large information spaces," *Inf. Syst. Res.*, vol. 7, no. 1, pp. 111–134, 1996.

[24] P. Weil and M. Broadbent, "Leveraging the new Infrastructure," *Harv. Bus. Sch. Press Boston*, 1998.

[25] K. Croman *et al.*, "On Scaling Decentralized Blockchains," in *Proc. 3rd Workshop on Bitcoin and Blockchain Research*, 2016.
[26] M. Pilkington, "Blockchain Technology: Principles and Applications," *Res. Handb. Digit. Transform. Ed. F Xavier Olleros Majlinda Zhegu Edw. Elgar*, 2016.
[27] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, 1997.
[28] A. Back *et al.*, "Enabling blockchain innovations with pegged sidechains," *URL Httpwww Opensciencereview Compapers123enablingblockchain-Innov.--Pegged-Sidechains*, 2014.
[29] O. Hanseth and K. Lyytinen, "Theorizing about the design of Information Infrastructures: design kernel theories and principles," *Sprouts Work. Pap. Inf. Environ. Syst. Organ.*, vol. 4, no. 4, pp. 207–241, 2004.
[30] J. H. Saltzer, D. P. Reed, and D. D. Clark, "End-to-end arguments in system design," *ACM Trans. Comput. Syst. TOCS*, vol. 2, no. 4, pp. 277–288, 1984.
[31] A. Antonopoulos, *The Internet of Money*. Merkle Bloom LLC, 2016.
[32] 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.
[33] 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,'" *Underst. Infrastruct. Dyn. Tens. Des.*, 2007.
[34] D. G. WOOD, *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER*. Ethereum, 2014.
[35] J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," Technical Report (draft). https://lightning. network, 2015.
[36] J. L. Zittrain, "The generative internet," *Harv. Law Rev.*, pp. 1974–2040, 2006.
[37] V. L. Lemieux and V. L. Lemieux, "Trusting records: is Blockchain technology the answer?," *Rec. Manag. J.*, vol. 26, no. 2, pp. 110–139, 2016.
[38] UK Government Office for Science, "Distributed Ledger Technology: beyond block chain," Government Office for Science, London, Jan. 2016.
[39] Lantmäteriet, "'Framtidens husköp i blockkedjan' ('Future real estate trade through the blockchain')," Lantmäteriet, Jun. 2016.
[40] M. L. MIT Media Lab, "Blockcerts-An Open Infrastructure for Academic Credentials on the Blockchain," *Medium*, 24-Oct-2016. .
[41] MIT Media Lab, "What we learned from designing an academic certificates system on the blockchain," *Medium*, 02-Jun-2016. .
[42] S. Eskandari, J. Clark, D. Barrera, and E. Stobert, "A first look at the usability of bitcoin key management," 2015.