

BEYOND BITCOIN

Public Sector Innovation Using the Bitcoin Blockchain Technology

Svein Ølnes, Vestlandsforskning (Western Norway Research Institute), sol@vestforsk.no

ABSTRACT

The virtual currency Bitcoin has got a lot of attention since it was presented in late 2008 and implemented in early 2009. However, the main attention has been on the currency and not the underlying technology called the blockchain. This paper argues that we need to look beyond the Bitcoin currency and investigate the potential use of the blockchain technology also for public sector as a mean for a secure, distributed, open, and inexpensive database technology. The technology is discussed as an information infrastructure and the generativity it allows and supports. After a thorough overview of academic publications on the subject of Bitcoin, and especially Bitcoin used in public sector, the paper presents a relevant use case highlighting the innovation potential of the new, distributed technology. The literature review reveals that the Bitcoin technology is absent from the e-Government literature, despite the undeniable high innovation potential it represents also in public sector. The use case presented shows that Bitcoin could be a promising technology for many types of permanent, or relatively permanent, documents in public sector.

Keywords: e-Government, digital government, bitcoin, blockchain, innovation, 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 made possible with the Bitcoin protocol holds a bit of the same potential as the aforementioned examples and comparison with the early web development has been done (Andreessen, 2014).

Public sector faces a number of challenges, not least in more cost efficient use of ICT and better interoperability between systems (Codagnone and Wimmer, 2007). The Bitcoin blockchain can be viewed as an open, distributed, and trustless database on the Internet. Trustless here means that it requires no third party to secure transactions. Currently the Bitcoin blockchain is limited to handle a maximum of seven transactions pr. second (Zohar, 2015) 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 typical a couple of cents) combined with a high degree of security makes promises for a cost efficient and secure way of storing also public documents of various types and in addition get a better interoperability due to the open and distributed architecture.

While technology adoption and efficient use in e-Government is a subject comprising far more than just technology itself, as for instance Welch and Feeney point out in their technology-organization capacity model (Welch and Feeney, 2014), a prerequisite for better use of ICT in public sector nevertheless is first a knowledge of what technologies are at hand, and then a discussion on how to best use them and incorporate them in the organizational structure.

So far there seems to be little discussion of this major technological breakthrough in public sector and what it can do for future development in e-Government. The research objective of this paper thus is

- to give an overview of the Bitcoin literature in general and Bitcoin 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 explore a use case that will shed light on the possible use of the technology in public sector. Bitcoin is used throughout the paper as a proxy for cryptobased currency systems. Bitcoin is by far the most important of these and represents in early 2015 a total market cap of approximately 3.5 billion US \$ (Böhme et al., 2015), more than 10 times the second most popular crypto currency platform (Ripple)¹.

In section 2 a brief explanation of the Bitcoin technology is given, to the extent necessary for the paper. In section 3 Bitcoin as an information infrastructure and platform for innovation is discussed in the context of public sector e-service development. The method used in the paper is described in section 4 before a use case is explored and discussed in section 5. Finally, section 6 concludes with open problems and suggestions for further research on the use of this quite important technology.

2 WHAT IS BITCOIN?

Bitcoin is a virtual currency first presented in a white paper by Satoshi Nakamoto (Nakamoto, 2008). As many will know, Satoshi Nakamoto is a pseudonym and the real author(s) and creator(s) have yet to be identified. The Bitcoin application was launched on the 3rd of January 2009 to a group of subscribers of a cypher-punk mailing list (Popper, 2015). For a couple of years not much happened to the new currency and activity was constrained to a small group of experts on cryptography that also happened to be deeply sceptical to the government (ibid.). But from 2012 on the interest in Bitcoin started to rise and reached a till now top in the end of 2013 and beginning of 2014. The sharp rise in exchange rates between Bitcoin and traditional currencies was the main reason for the increasing interest. However, what goes up, generally must come down, and the downfall in exchange rates was substantial. From January 2014 to the end of the year the Bitcoin to US dollar exchange rate fell from ca. 950 US \$/BTC to ca. 250 US \$/BTC. Throughout 2015 the exchange rate has been relatively stable and in the range of 2-300 US \$/BTC².

Digital cash was nothing new when Bitcoin entered the stage in 2009. David Chaum introduced the concept in 1983 and at the same time he introduced blind signatures to prevent payments to be traceable (Chaum, 1983). But the requirement of a central server to hold the signatures was the Achilles' heel and continued to be so until the advent of Bitcoin. Other noticeable contribution to the development of digital cash, or crypto currencies, was done by Adam Back with *Hash cash* (Back, 2001), Nick Szabo with *Bit gold* (Szabo, 2008), and Wai Dei with *b-money* (Dai, 1998). Bitcoin builds on all these efforts (Popper, 2015).

Bitcoin was the first technology to solve the problem of how to establish trust between otherwise unrelated parties over an untrusted network like the Internet without relying on a third, central party, be it organisational or technological. The problem of establishing trust among untrusted parties is generally known as the Byzantine Generals' Problem and was first formulated by Lamport et al. (1982). 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, trust which message is the correct one when it gets conflicting messages?

The problem was illustrated with the story of a Byzantine army camping outside an enemy city. The generals can communicate with one another only by messenger. They must decide on whether to attack or withdraw, but the problem is that there could be traitors among the generals preventing the loyal generals from reaching a conclusion. Is there an algorithm that can help the majority of the generals (the loyal generals) to reach a conclusion without being disturbed by the traitors? Bitcoin solved the problem in an elegant way by using a method based on "Proof-of-work" (Nakamoto, 2008). To put it simple: to compromise the system by trying to alter the transactions on the blockchain will cost enormous amounts of computing power, which translates into electrical power and that means a lot of money. The cost of compromising the system must outweigh the profit of doing so.

¹ <http://coinmarketcap.com>

² <http://bitcoincharts.com>

Bitcoin is a distributed technological platform that is both a currency and an underlying infrastructure for moving virtual money or other digital things. The unique feature of Bitcoin is that it facilitates payments between persons or parties without the need for a trusted third part. Trust is built into the technology and is maintained by the network of Bitcoin users. This represents a major technological breakthrough and at the same time also threatens to disrupt existing structures built on third party trust, like our banks. There is no central bank issuing new bitcoins as there are no banks guaranteeing payments between individuals.

In addition to solving the trust problem formulated in the Byzantine generals' problem in a technological way Bitcoin also has introduced other remarkable features: It is the first technology realizing micro payments and it is also the first technology to combine a currency and secure deposits of digital assets; preferably assets that do not change over time or that changes very little. The last feature is the base for this paper and the use case described in section five.

The most interesting thing with Bitcoin seen from a public sector view thus is the blockchain technology. It is a public ledger where all Bitcoin transactions are recorded – free for everyone to access. The details of a transaction do not reveal directly the parties involved, only the addresses of the involved parties and the amount of Bitcoin transferred (Antonopoulos, 2014). 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. One cannot exist without the other (ibid.).

Bitcoin relies on two fundamental technologies from cryptography (Böhme et al., 2015): public-private cryptography for making digital signatures to store and spend money and cryptographic validation of transactions by hash functions. A Bitcoin transaction is a digital signature which signs a transaction containing the payers address, the recipients address, and the amount (of bitcoin) transferred (Antonopoulos, 2014). 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 a single 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 part. The one who solves the puzzle first gets 25 BTC³ in reward⁴.

The mining operation and the following bitcoin reward is the only way new bitcoins are released into the system, and is an important incentive to the miners and their securing of transactions. Of special interest for the use of Bitcoin technology in public sector is so-called sidechains. There already exist many alternative blockchains to Bitcoin. These are blockchains sharing the underlying Bitcoin technology, but differing in addresses (Back et al., 2014). From the alternative chains we have alternate coins, or *Altcoins*. Back et al. (ibid.) introduces the concept of *pegged sidechains*, which are interoperable blockchains where assets can be moved freely between chains. Instead of using the main Bitcoin blockchain for all sorts of transactions they propose pegged sidechains to ease the pressure on the main block and to achieve better security by partly isolating transactions that are not strictly about payments between parties. A major benefit of sidechains compared to alternative chains (Altcoins) is that the sidechains use Bitcoin and can use the PoW work done on the main blockchain for security. The currency Bitcoin is also transferrable between the main blockchain and the sidechains. Another important factor is that the amount of money at risk is only the money in the sidechain, not the money in the main blockchain (Back et al., 2014).

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 is a platform on which new applications and services can be built. The Internet itself represented, and represents, an important platform for permissionless innovation both in private and public sector, and the Bitcoin infrastructure holds the same promises in its field.

³ BTC is the current notation of the Bitcoin currency (1 BTC = 1 Bitcoin)

⁴ The reward started out with 50 BTC and was halved in 2012 to 25 BTC. It will be halved again in 2016 and follows this scheme until all 21 mill. Bitcoin have been released. By the year 2140 all bitcoin will be released, and reward for the miners will be reduced to the fees included in the transactions (Nakamoto, 2008).

3 BITCOIN AS AN INFORMATION INFRASTRUCTURE FOR PUBLIC SECTOR INNOVATION

Bitcoin can be seen as an information infrastructure in that it meets the definition “*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*” (Hanseth and Lyytinen, 2010). The characteristic properties of an information infrastructure and how Bitcoin fits in is showed in the table below. The table builds on Hanseth and Lyytinen (ibid.).

Table 1: Bitcoin as an information infrastructure

Property	Information infrastructure (in general)	Bitcoin as an information infrastructure (II)
Shared	Universally and across multiple IT capabilities	Bitcoin is universally shared (one only need an Internet connection to use/take part)
Open	Yes, allowing unlimited connections to user communities and new capabilities	Bitcoin is open for any users and offering an infrastructure for “permissionless innovation”
Heterogenous	Increasingly heterogeneous both technically and socially	Bitcoin has already generated a myriad of new applications and platforms (hundreds of altcoins, emerging sidechains, foundation for new platforms like Ethereum ⁵)
Evolving	Yes, unlimited by time or 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	Bitcoin itself is fairly new (6,5 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 (WOOD, 2014), (Poon and Dryja, 2015)
Control	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)

Although Hanseth and Lyytinen distinguish between platforms and an information infrastructures, Bitcoin can also be seen as a digital platform, as defined by Kazlan et al. (Kazan et al., 2014). Their definition, which builds on Yoo et al. (Yoo et al., 2010) reads: “a proprietary or open modular layered technological architecture that support efficient development of innovative derivatives”. Digital platforms thus differ from other other central ICT concepts like *architecture* and *infrastructure*. Architecture is the conceptual and logical structure of a system (Tiwana et al., 2010) whereas infrastructure is the operationalisation of architecture (Hanseth and Lyytinen, 2010). Despite these differences Bitcoin regarded as a platform in Kazan et al.’s view (2014) can also help us understand the use of the technology in public sector.

⁵ Ethereum is a derivative of Bitcoin that focuses on smart, programmable contracts. It uses a separate blockchain with its own currency; ether (WOOD, 2014)

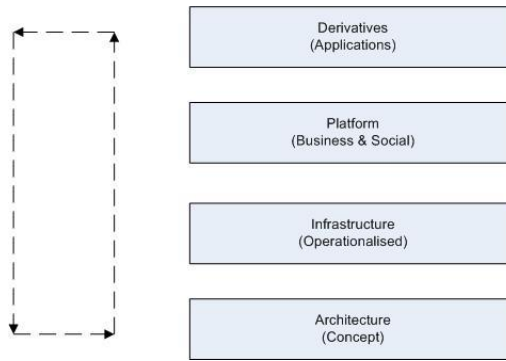


Figure 1: Platform Evolution (Kazan et al., 2014)

The digital platform part is again divided in layers, from bottom and up: 1) Device layer, 2) System layer, 3) Network layer, 4) Service layer, and 5) Content layer (Kazan et al., 2014). Although Kazan et al. investigates digital platforms as disruptive information technology artefacts in a business context, the model will also suit public administration and public sector service provision. Kazan et al. also introduce the governance regime as another dimension to the platform dimension. They differentiate between a centralised and decentralised governance regime and argue that the strategic interplay of governance regimes and platform layers is deterministic of whether disruptive derivatives are permitted to flourish. They use the PayPal service (centralised governance) and Coinkite (decentralised governance) in their comparative use cases study. CoinKite is a Bitcoin wallet.

This paper recognizes the digital platform and governance regime interplay as an important factor for disruptive derivatives to be developed. The paper also builds on the assumption that the governance model in public administration is centralised, and that introducing a new digital platform like Bitcoin could foster new disruptive derivative services in public sector, but at the same time could challenge the centralised governance model. The disruptive derivatives will rely on the technology's generativity, as defined by Zittrain (2006). According to Zittrain generativity denotes a technology's overall capacity to produce unprompted change driven by large, varied, and uncoordinated audiences. He contrasts generativity to openness and argues that a pc running the Windows operating system (OS) is highly generative despite the proprietary nature of the OS. Zittrain's ideas of generativity corresponds very much to the information infrastructure theory, but lacks the theoretical underpinning (Hanseth and Lyytinen, 2010).

The use case presented in section five will be discussed in light of digital platforms, information infrastructures, and the ideas of generativity.

The research objective of the paper is to show that the Bitcoin technology represents a valuable digital platform for generativity and innovation also in public sector. This will be shown by exploring a use case to shed light on the innovation potential in public sector, but first we will give an overview of the Bitcoin literature in general and the Bitcoin literature in public sector especially.

4 METHODOLOGY

The paper is of explorative and conceptual nature and relies on a thorough literature review of public sector related Bitcoin papers. 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. The only part of Bitcoin paid attention to by public sector is understandably the regulation concerning the currency.

Although Bitcoin is built on well-known technology it is a new platform with few implementations and none based on public sector services, as far as this author has managed to identify. The paper therefore

must be based on existing literature where public sector and e-Government is mentioned, and pilots involving public sector based services or related to public sector. The first few academic publications on Bitcoin emerged in 2011, and the number has subsequently grown by a factor of around three since then, as Brett Scott's overview shows (Scott, 2014):

Table 2: The growth of academic publications with Bitcoin as a theme (Scott, 2014)

Year	No. of publications
2011	8
2012	21
2013	63
2014	208

Table 2 shows that the number of academic publications (most of the publications are peer-reviewed papers) grows exponentially. But it also shows that the number of academic publications is relatively small. Due to this fact "white papers" have been an important source of information for those who want to learn about the technology and the possibilities. A white paper is "an authoritative report or guide informing readers in a concise manner about a complex issue and presenting the issuing body's philosophy on the matter"⁶. Although white papers often come close to marketing presentation, many of the Bitcoin white papers resembles academic papers (e.g. Satoshi Nakamoto's original Bitcoin paper (Nakamoto, 2008) and Adam Back et al.'s paper on side chains (Back et al., 2014)).

The main source of literature for the topic Bitcoin in e-Government is the extensive e-Government Reference Library, EGRL, which in the latest version 10.5 contains 7,237 of predominantly English-language, peer-reviewed work in the study domains of electronic government and electronic governance (Scholl, 2015) and the Google Scholar academic search tool.

Furthermore, the list of Bitcoin-related academic publications assembled by Brett Scott (Scott, 2014) has been used to identify relevant papers. The table below shows a categorization of the papers found using the three sources. Broad categories of technology, economy, regulations, and e-government were created as a result of screening the Bitcoin related papers. The categorization was done based on the title, the summary of the papers, and the journal. In case of ambiguity the complete paper was downloaded.

Table 3: Categorization of Bitcoin publications from different sources

Category	EGRL 10.5	Google Scholar	Bitcoin Academic Publ.
Search phrase ⁷	"bitcoin"	"bitcoin e-Government"	-
Economy	0	1	114
Technology	0	1	124
Regulation	0	4	59
Other	0	0	17
Irrelevant	-	78	0
Total	0	84	314

Searches for "bitcoin" in the extensive e-Government literature database EGRL 10.5 did not give any result, a clear indication that the research community in the e-Government field has not yet discovered or considered this topic. A search for "bitcoin" and "e-Government" on Google Scholar did give 84 results, but most of them turned out to be irrelevant. Only six publications dealt with Bitcoin or crypto currencies

⁶ Wikipedia: https://en.wikipedia.org/wiki/White_paper

⁷ For the collection Bitcoin Academic Publications all publications were categorized.

and four of them was about regulations. The two papers categorized as ‘Technology’ and ‘Economy’ did not really fall into the e-Government field despite the mentioning of ‘e-Government’. The best source for academic literature on Bitcoin is the Bitcoin Academic Publications, assembled by Brett Scott (Scott, 2014). It is an extensive coverage of Bitcoin related publications published in a Google spreadsheet open for everybody. It is updated to include 2014 publications. Most of the publications listed fall within the fields of technology and economy. There are also quite a few publications dealing with 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. It is high time to do something about that.

We have also used a case study approach (Yin, 2013) 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 (Yin, 2013, Kazan et al., 2014). This is the case for Bitcoin in e-Government context where there to date are no obvious use cases to study.

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 (Antonopoulos, 2014). In addition to serving on the advisory board for many startup companies in Bitcoin technology he is also a Teaching Fellow at the University of Nicosia where he teaches the online courses in digital currencies. Finishing the MOOC-based⁸ 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 (University of Nicosia, 2014). 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 information assets, not just as a currency or a payment system. 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:

- The process should involve no other services or products other than the Bitcoin blockchain
- The process should allow someone to authenticate a University of Nicosia certificate without having to contact the University of Nicosia
- The process should allow someone to complete the process even if the University of Nicosia no longer existed (or, more likely, if the University of Nicosia website no longer existed in its current form or records are lost and so on)

The process of storing the academic certificates on the blockchain followed these steps (University of Nicosia, 2014):

1. 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 (Schneier, 1994). In addition to the one-way function (there is no way to recreate the document given the hash value of it), another important property of hash functions is that the risk of two different inputs generating the same hash value is practically non-existent. Also the slightest change in the input text (e.g. removing a comma) will produce a completely different hash value of the docu-

⁸ MOOC = Massive Open Online Courses

ment. Hash functions are generally used to verify the integrity of messages. In Bitcoin technology the SHA-256 hash function is used. The SHA-256 hash function belongs to the SHA-2 collection of functions designed by the National Security Agency (NSA) to be a new standard, replacing the SHA-1 collection (Liu and Özsu, 2009).

2. **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 (see Appendix). The reasons for doing it this way were both effectiveness (less waste of blockchain space) and security (more secure than individual certificates). 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.

3. **Timing and instructions**

The certificates had to be self-verifying and it created a problem with the entering of the hashed index on the blockchain. The solution was to indicate a time frame in the documents and be very careful about the process until the certificates were placed on the blockchain.

4. **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:

1. **Verifying the index document**

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

2. **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 organisations 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 1. 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 (Hanseth and Lyytinen, 2010). 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 four. However, the legal and regulatory factors discussed in these papers are mostly about regulating the cur-

rency 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.

Bitcoin is often touted as a “trustless” technology because it does not rely on a third party to secure transactions. However, the term “trustless” is a bit misleading, and for several sectors, not least public sector, a term that could make the technology repellent. Trust is a part of all ICT systems, also peer to peer systems. The difference is that trust must be put in the developers and the network itself, rather than in a third party institution.

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 (Ness, 2013). Internet’s rise in popularity made it a de facto standard that soon overran the OSI protocol’s, 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 model that Internet itself.

There is also the question of the strategic interplay of governance regimes and platform layers and its influence on the flourishing of disruptive derivatives according to Kazan et al. (2014). If this is also the case for public sector services is unclear and something worth following up through more research. This is highly connected to the generativity potential of the Bitcoin technology as an open, permissionless innovation platform.

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.

The use case detailed and analysed in the chapter above shows that Bitcoin indeed should be of interest also for public sector bodies. 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.


e-Government researchers must wake up and see the promising potential in the Bitcoin technology and start researching ways this technology can be utilized by public sector. This topic is wide open for research. 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? Finally, are the generativity factors of the Bitcoin technology sufficiently met in order to foster innovation also in e-Government service development?

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 could approach the Bitcoin technology.

References

- Andreessen, M., 2014. Why Bitcoin Matters.
- Antonopoulos, A.M., 2014. Mastering Bitcoin - Unlocking Digital Cryptocurrencies, 1st ed. ed. San Francisco.
- Back, A., 2001. Hash cash: A partial hash collision based postage scheme. URL <http://www.hashcash.org>.
- Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., Wuille, P., 2014. Enabling blockchain innovations with pegged sidechains. URL: <http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains>.
- Böhme, R., Christin, N., Edelman, B., Moore, T., 2015. Bitcoin: Economics, Technology, and Governance. *The Journal of Economic Perspectives* 29, 213–238.
- Chaum, D., 1983. Blind signatures for untraceable payments, in: *Advances in Cryptology*. Springer, pp. 199–203.
- Codagnone, C., Wimmer, M.A., 2007. Roadmapping eGovernment Research: Visions and Measurestowards Innovative Governments in 2020. Guerinoni Marco.
- Dai, W., 1998. B-money. Consulted 1, 2012.
- Hanseth, O., Lyytinen, K., 2010. Design theory for dynamic complexity in information infrastructures: the case of building internet. *Journal of Information Technology* 25, 1–19.
- Kazan, E., Tan, C.-W., Lim, E.T., 2014. Towards a Framework of Digital Platform Disruption: A Comparative Study of Centralized & Decentralized Digital Payment Providers. ACIS.
- Lamport, L., Shostak, R., Pease, M., 1982. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)* 4, 382–401.
- Liu, L., Özsu, T.M., 2009. *Encyclopedia of Database Systems*. Springer US.
- Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. Consulted 1, 28.
- Ness, B., 2013. Tilkoplet - En fortelling om Internett og Forskningsnettet i Norge. Fagbokforlaget.
- Poon, J., Dryja, T., 2015. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Technical Report (draft). <https://lightning.network>.
- Popper, N., 2015. *Digital Gold - Bitcoin and the Inside Story of the Misfits and the Millionaires Trying to Reinvent Money*, 1st ed. ed. HarperCollins, New York, NY, USA.
- Schneier, B., 1994. *Applied Cryptography—Protocols, Algorithms, and...*
- Scholl, H.J., 2015. eGovernment Reference Library (EGRL) version 10.5.
- Scott, B., 2014. Bitcoin Academic Research. *The Heretic's Guide to Global Finance: Hacking the Future of Money*.
- Szabo, N., 2008. Bit gold. Website/Blog.
- Tiwana, A., Konsynski, B., Bush, A.A., 2010. Research commentary-Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics. *Information Systems Research* 21, 675–687.
- University of Nicosia, 2014. Academic Certificates on the Blockchain [WWW Document]. MSc in Digital Currency - University of Nicosia. URL <http://digitalcurrency.unic.ac.cy/certificates> (accessed 7.1.15).
- Welch, E.W., Feeney, M.K., 2014. Technology in government: How organizational culture mediates information and communication technology outcomes. *Government Information Quarterly* 31, 506–512.
- Wood, D.G., 2014. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum. <http://gavwood.com/paper.pdf>
- Yin, R.K., 2013. *Case Study Research: Design and Methods*. SAGE Publications.
- Yoo, Y., Henfridsson, O., Lyytinen, K., 2010. Research commentary-The new organizing logic of digital innovation: An agenda for information systems research. *Information Systems Research* 21, 724–735.
- Zittrain, J.L., 2006. The generative internet. *Harvard Law Review* 1974–2040.
- Zohar, A., 2015. Bitcoin: under the hood. *Communications of the ACM* 58, 104–113.

APPENDIX: Excerpts of the index document and the hashed certificates from the course in digital currencies, University of Nicosia, 2014

**UNIVERSITY OF NICOSIA**

INDEX OF CERTIFICATES AWARDED TO THE STUDENTS WHO SUCCESSFULLY COMPLETED THE DFIN-511 INTRODUCTION TO DIGITAL CURRENCIES COURSE OF THE UNIVERSITY OF NICOSIA'S MSc IN DIGITAL CURRENCY, JULY-SEPTEMBER 2014

A SHA-256 hash of this index document has been stored in the Bitcoin blockchain on September 15th 2014, in a transaction that will also be announced on September 15th 2014 through University of Nicosia's website and Twitter account @MScDigital.

On the following pages are the SHA-256 hashes of the 137 certificates awarded to the students who successfully participated in the DFIN-511 Introduction to Digital Currencies MOOC, offered by the University of Nicosia.

To verify the authenticity of a presented certificate, please follow these steps:

(1) Confirm the authenticity of the index document:

- (a) Ensure that you are using a valid index document supplied by the University of Nicosia
- (b) The index document PDF can be found at <http://digitalcurrency.unic.ac.cy/certificates> and at other online locations distributed by the University of Nicosia
- (c) The validity of the index document can be confirmed by reviewing the OP_RETURN field in blockchain transactions confirmed between 1200 and 1400 GMT on September 15th 2014. The SHA-256 hash of the valid index document, prepended by "UNICDC " (554e6963444320 in hex encoding) will be found in one transaction during that period

(2) Confirm the authenticity of the certificate:

- (a) Produce a SHA-256 hash of the PDF certificate to be authenticated
- (b) Search for the certificate's SHA-256 hash within the authenticated index document. If the hash code is found, then the certificate is authentic

CERTIFICATES OF ACCOMPLISHMENT

Certificates of Accomplishment were awarded to the students who attempted and completed at least 75% of all quizzes and achieved a grade of 60% or above on the final exam of the DFIN-511 Introduction to Digital Currencies MOOC

113 certificates awarded

```
4234ef753e32ef88e7a9136266dccb1e5e53df51eb6dade7c9dfe0c13a4b0c381
8a1eb27d0310073a4248bd85ca94eee5a715d9013fb907014fd16779eb875001
b3c01ef80eca962af767273285c759399a9a7f55021a3c7a567feae549e09a31
5caa5898eadcef4d39ccc7e9ef7d7fc05f5761c5dfc0b3d6874e0d355a1dd03
d63adec2081a7e5289f47d434f7f456373a6e978d8e6efb4156d86b42030bd68
c175d38f3c449eabf58b0da64855d5471425ad9c9b5a07c2f63a7f9f4ca76d0e
002aed890d6aa8e5d19a8cf12b4dd03b487812d9cf62f576c6d83ab0afe6c866
6d12e1bb9db23c1caa5025f7e5da6c08256f6e92f2588c7040aa33714b8418a6
2eab8ba4919968927b60c8abe3d5bb0424a47cddc80dc1bbec668e43886b8f93
71a5a9bf5d9f2dc9d04b44e872100cb2f399a7fa9c3b8e44e8c822c04c30f0cf
b7302fa8148ed6f359369533b850e34f4e34d1fcddeb9c4541ce11e7e89629177
b2335d826c18758b86bbec0aba775091a2c19c8f229c53016171a4384b90fefb
96f6d5bedf9574cc195208d85e7b5bc614c18c41092b58fa8118778c036a1b5b
e808b3cf9e674231aec8ef75187f3f109534fb33f0a5f47c8ad9280a818dc0bd
b5a26a088be3d3a5e1a5cd49cc07c15d11c7dc55b46b522e26c8943be12917c6
9810e6ff5d0dadf25d33e1150c9a45971d8826c2a27e517b4f822bb6289da8e9
bf40209290da18c188e976060cb1fbff47ff79b763502f6c7562cb5adff76d0
1a75dce28cb1441143820f45a00c6df6e54bc6e88f5a01760d3f1bc1ca4cecb3
83c73abdc3dfd1c7b05b545091c0b80804302beeea602f7483d3ed1e3c9e85f9
c30c61056f6bd11654c30dc9c9ba18d533e44ec2ff72ce15509c7ee892044df6
43205c6ca6538ed1e06b3224a21687b528533f4fc619f7a7f3cd2e05c77dd1ff
cb0f504f6697208cedc76a4226c5a12811e19c5a79f65e6938844d075f1e5396
7a3faad96dd66cbfcc5f78cb0163a130197aeeb5719eb256c5abdbad01d31540
a5079b7b1cc82bf40e4a39ca3c65f017fb5eb43241bb56d3bb7083f38f5dfeb
751359334a0c170e22e5c2d629e2b846efc156afe4a4d3953b880455dfda75a4
```