OXFORD

Policy and Society, 2022, **00(0)**, 1–16
DOI: https://doi.org/10.1093/polsoc/puac014
Original Research Article

Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia

Silvia Semenzin[1], David Rozas[1] and Samer Hassan[1,2]

[1]GRASIA Research Group, Institute of Knowledge Technology, Complutense University of Madrid, Madrid, Spain
[2]Berkman Klein Center for Internet & Society, Harvard University, Cambridge, MA, USA
Corresponding author: S. Semenzin, Faculty of Computer Science, Department of Software Engineering and Artificial Intelligence, Complutense University of Madrid, Avenida del Prof. José García Santesmases, 9, Madrid 28040, Spain.
Email: ssemenzi@ucm.es

Abstract

Blockchain technology enables new kinds of decentralized systems. Thus, it has often been advocated as a "disruptive" technology that could have the potentiality of reshaping political, economic, and social relations, "solving" problems like corruption, power centralization, and distrust toward political institutions. Blockchain has been gradually gaining attention beyond finance and is thus applied by a range of different actors. This includes local, regional, and national governments interested in the potentiality of experimenting with blockchain-supported governance. This article contributes to identifying blockchain as a contested socio-political object prone to contradictory political imaginaries regarding its potentialities, particularly when applied to policy. The article explores some of the most praised of blockchain's affordances (e.g., decentralization and transparency) in the context of Estonia, one of the most cited examples of blockchain governmental applications. Estonia has received international attention as the alleged first national infrastructure integrating blockchain. However, so far, few have asked: what kind of blockchain-based tools have been built by the Estonian government in practice and why? And to what extent do blockchain-based governmental applications reflect the original promises of disruption of the crypto-community? This article draws on a qualitative approach to explore several blockchain-based socio-technical objects to identify the narratives that have emerged in Estonia. The research shows clear contrasting views between stakeholders and technical experts from inside and outside the institutional sphere. The conflict revolves around two different social imaginaries associated with permissioned vs. public blockchains. The paper concludes with an analysis of the profound political implications of each vision.

Keywords: blockchain; case study; E-Estonia; governance; imaginaries

In October 2008, a whitepaper published under the pseudonym Satoshi Nakamoto described the functioning of Bitcoin (Nakamoto, 2008): a cryptocurrency which, for the first time, operated exclusively under a decentralized infrastructure. Over the next few years, Bitcoin attracted increasing media attention and grew in popularity, in parallel with its economic value relative to standard currencies such as the US dollar (Columbia, 2016). Beyond the financial innovativeness of Bitcoin as a cryptocurrency, technological enthusiasts soon realized what was truly innovative about Bitcoin: the underlying infrastructure known as a blockchain.

Blockchain became known as a "disruptive" technology since it provides novel affordances to avoid centralized data storage and execution of instructions, contrary to the Web as it is currently. The concept of a distributed ledger is advocated as a new kind of technology that ensures horizontal, safe, and transparent transactions: blockchain makes a tamper-evident public ledger of transactions possible, without the need for any central authority, and allows multiple actors in a network to record, verify, or share data on a peer-to-peer basis (Pólvora et al., 2020).

In recent years, blockchain has gained growing attention from various actors (Hassan et al., 2020), including governments and international organizations interested in the potentiality of experimenting with blockchain-supported governance (Faqir-Rhazoui et al., 2021). At an institutional level, blockchain potentials are envisioned to avoid power centralization problems on the Internet, tackle corruption, and increase governmental transparency (Tapscott & Tapscott, 2016). However, these views clash with the original "promises" of Bitcoin and blockchain, which arose from the crypto-anarchist community who envisioned blockchain as a way to eliminate intermediaries and central actors (Filippi & Hassan, 2016).

The Estonian government was an early institutional adopter of the technology (Novak, 2019, 178), and it is usually presented as one of the most well-known actors in the experimentation with blockchain-based technologies in the public sector (Alexopoulos et al., 2021). As part of the project E-Estonia, the Estonian government decided to incorporate blockchain-based applications into their digital infrastructures (Galen et al., 2018; Tan et al., 2020). Despite the novelty represented by Estonian's use of blockchain technologies at a governmental level, a lack of research analyzing how they have been employed remains. By drawing on the case of Estonia, this article examines how blockchain technology is being narrated within the public and institutional spheres and discusses the extent to which governmental applications of blockchain could create "societal disruption" (Christensen, 2006).

Through this in-depth exploration of blockchain-based governmental projects, we reveal how the discourse on blockchain technology exhibits a certain interpretative flexibility (Pinch & Bijker, 1984). We identify a lack of universal agreement on essential concepts surrounding blockchains and their effects on institutional contexts. This ambiguity results in blockchain becoming a source of multiple, and often contradictory, socio-technical imaginaries (Jasanoff & Kim, 2015). Our results show how blockchain becomes a contested issue both in its technical and conceptual dimensions, leaving room for broad interpretations of the same technology, which entails a struggle for gaining hegemony in the public discourse.

First, we examine work related to the myriad of blockchain interpretations and focus, subsequently, on those regarding its affordances for blockchain-based governance. Secondly, we discuss our case study and an overview of the blockchain narratives and political imaginaries surrounding it. We then introduce the research methodology and data collection methods employed in the study. Finally, we present and discuss our results, in which we analyze transparency and decentralization as affordances prone to narrative clashes inside blockchain interpretations.

Blockchain: a myriad of perspectives

In simple terms, a blockchain can be understood as a permanent and distributed collection of data that is visible and verifiable to everyone in the system. In the case of Bitcoin, the blockchain stores transactions between individuals willing to engage in economic exchange. The process is supported by a novel form of cryptography that ensures pseudo-anonymity and does not require the intermediation of a central authority (Huckle & White, 2016; Nakamoto, 2008). In other words, the history of transactions generated by using cryptocurrencies can be stored in a blockchain without the need to trust a third party, such as a bank server. Over time, more generic blockchain-based platforms (Macdonald et al., 2017) have emerged, fostering the use of blockchains beyond cryptocurrencies. For example, in the context of medical and healthcare applications (Kuo et al., 2019).

From a technical perspective, blockchains can be conceptualized as ledgers that enable the implementation of novel properties at an infrastructural level in a fully decentralized manner. A ledger is "a chain of cryptographically linked 'blocks"' (Hileman & Rauchs, 2017, 11). In this chain, each block depends on the information stored in the previous block. Another key characteristic of blockchain, related to this technical perspective, is its capacity for distributed computation. In a blockchain, computation is executed collectively by all the nodes of the system. As a result, blockchains are resistant to tampering (Atzori, 2015). In other words, if a node in the network tries to tamper a block with its own version of the blockchain, the successive blocks' hash functions will also change (Primavera & Loveluck,

2016), and the block will be considered invalid. In blockchain terminology, this process is known as a "proof-of-work".

Blockchains are also conceptualized as open networks in which individuals are not required to know each other prior to engaging in a transaction. On the basis of this conceptualization, some authors have argued that blockchains can be understood as a type of peer-to-peer "trustless" technology (Atzori, 2015; Gerard, 2017; O'Dwyer, 2015; Tapscott & Tapscott, 2016). Thanks to the novelty of the cryptographic primitives, the electronic transactions stored in the blockchains are automatically verified by the nodes of the network they belong to. Therefore, the system does not require intervention from a third party in order to execute the action. Antonopoulos (2014) argues the "trustless" characteristic of blockchain systems poses "a shift from trusting people to trusting math". A similar emphasis is placed, for example, on Bitcoin's whitepaper: describing proof-of-work as a mechanism that enables algorithmic auto-regulation (Nakamoto, 2008), leaving traditional forms of trust which rely on social confidence obsolete.

Finally, blockchains have also been conceptualized as socio-technical objects which enable the exploration of potential affordances to experiment with (e.g., Cila et al., 2020; Fritsch et al., 2021; Rozas, Tenorio-Fornés, Díaz-Molina, et al., 2021; Rozas, Tenorio-Fornés, Hassan, et al., 2021). Drawing on this conceptualization, Rozas, Tenorio-Fornés, Díaz-Molina, et al. (2021) identified six potential affordances of blockchains. Firstly, tokenization (1): the use of blockchains to transform the rights to perform an action on an asset into tokens. Secondly, self-enforcement and formalization of rules (2): the capacity to embed organizational rules into smart contracts. Thirdly, autonomous automatization (3): defining complex sets of smart contracts that allow multiple parties to interact with each other without human interaction. Fourthly, an affordance to communalize the ownership and control of the technological objects: decentralization of power on the infrastructure (4). Fifthly, the blockchain's capacity to increase transparency (5) by relying on its immutability properties. Finally, an affordance for a partial codification of trust (6), which facilitates agreements between agents without requiring a third party. This conceptualization of blockchains as socio-technical objects places the focus on the need to experiment with the potentialities of blockchain beyond the finance sector and cryptocurrencies. This experimentation with blockchains in different social fields is indeed already happening and rapidly expanding to diverse areas. According to a dossier compiled by the Stanford Business Center for Innovation (Galend et al., 2018), blockchain applications today exist in different contexts beyond finance. These include governance, philanthropy, digital identities, agriculture, and distributed energy utility systems, to name but a few. For blockchain enthusiasts, the fields of applications of this technology are potentially unlimited since blockchain "would enable the disintermediation of any digital transaction at a global level" (Atzori, 2015).

This article incorporates this myriad of conceptualizations of blockchains within the analysis of blockchains applied to the public and institutional spheres. Next, we will focus on the specific debates surrounding blockchain-based forms of governance to lay the groundwork for analyzing this connection with the original crypto-anarchist promises of creating "societal disruption" (Christensen, 2006) within this institutional context.

Blockchain-based governance and its narratives

The experimentation with blockchains to facilitate and scale up governance processes is increasingly attracting the attention of diverse fields of social sciences (e.g., Cagigas et al., 2021; Risius & Spohrer, 2017). Within the emergent literature on blockchain-based governance, we can find a significant contrast between the two streams. On the one hand, a set of hegemonic discourses (e.g., Hayes, 2016; Heuermann, 2015; Swan, 2015) inherently assumes that "anything that can be decentralized will be" (Johnston, 2014). This stream is influenced by the values of crypto-communities and so-called crypto-anarchist ideology (May, 1988): envisioning blockchain as an object to disrupt centralized forms of power and avoid intermediaries. It also encompasses libertarian views that strive to create an emerging global society without States and traditional institutions (Atzori, 2015; Golumbia, 2016).

On the other hand, we can find a critical stream that highlights the reductionist nature of the former (e.g., Atzori, 2015; Atzori & Ulieru, 2017). Within this stream, the counter-argument is that the massive adoption of blockchain services—without public institutions to coordinate them—may create new oligarchies and increase societal polarization (Primavera & Loveluck, 2016). This critical stream is commonly built upon the reinforcement of the role of central authorities in governance. As a result,

the potentialities of blockchain in this area are envisioned in ways that support the control required by institutional forms of governance. For example, to provide more transparency to the central institutions which operate in an institutional context (Nguyen, 2016) or more efficient mechanisms to control tax fraud (Ainsworth & Shact, 2016). In this stream, blockchain has been advocated as a potential solution to several issues from the datafied society (Schäfer & Van Es, 2017). These issues include: ensuring citizens' data ownership (Tapscott & Tapscott, 2016), the urge for privacy protection (Zyskind & Nathan, 2015), and demands to increase the degree of transparency of platforms (Catlow, 2017; Tapscott & Tapscott, 2016). The increasing number of policy documents and reports discussing blockchain-based governance published by several international policymakers, such as the European Union, the OECD, the United Nations, and the World Bank, to name a few, illustrates the relevance of this debate. The following excerpt, from a report by the World Economic Forum (2020, p. 4), provides an example of how blockchain could address corruption problems:

> *"[..] blockchain provides the unique combination of permanent and tamper-evident record-keeping, transaction transparency and auditability, automated functions with 'smart contracts', and the reduction of centralized authority and information ownership within processes. These properties make blockchain a high potential emerging technology to address corruption."*

At the end of 2018, it was estimated that more than 100 government-led blockchain projects were being trialed in more than 40 countries (Jun, 2018). Experimentation with blockchain in policy revolves around areas such as electronic voting systems, the management of land registers, recording and sharing medical information, the creation of e-ID, and more recently, even blockchain cities (ibidem). Overall, the power of blockchains for public interest resides in its advocated capacity to concurrently offer transparency, trust, and privacy, all desirable elements from a governance perspective. As a result, blockchain "in", "for", or even "against" government arises as an emerging field of study.

The concept of "blockchain" becomes in this sense a potentially powerful tool to be utilized in the public imagination. We draw on this clash between these different streams and their imaginaries to explore whether such experimental applications of blockchain at a governmental level are indeed fulfilling the promises of "disruption" or instead reinforcing centralized practices. In this sense, it becomes particularly relevant to delve into the imaginaries and the reasons for which governmental institutions, such as those in Estonia, are increasingly interested in incorporating blockchains into their digital infrastructure. Next, we provide an overview of this case.

The case of blockchain in Estonia

After restoring its independence in 1991, Estonia saw an enormous effort for modernization, which mainly resulted in several digital reforms throughout the 1990s. On entering the post-Soviet era, the country looked at the digital revolution as an essential source for attracting foreign investment and building international relations.

Over time, this translated into numerous reforms in terms of innovation and a number of different digitalization projects. In 2008, the Estonian government was announcing the birth of "E-Estonia", an ambitious project that aimed to digitalize all kinds of citizens' activities concerning the government. Although some research has outlined possible issues in terms of data privacy and social discrimination (Tammpuu & Masso, 2019) that may arise from the implementation of e-Estonia, the project is often publicly celebrated as a technology-based information society that establishes the principles of e-government (Kalvet, 2012a). This is due to the fact that almost all the public services in Estonia include an e-service component nowadays. The best-known example is e-Residency, launched in 2014, which consists of issuing a digital ID card that facilitates commercial activities within the Estonian public and private sectors (Sullivan & Burger, 2017). Other examples include mobility services, access to health and education records, and e-voting.[1]

Estonia is also claimed as one of the most advanced examples of a government using blockchain technology for enhancing institutional services (Galen et al., 2018, 22; Alexopoulos et al., 2021). Following the blockchain "hype" started in 2008, this contributed to fuel Estonia's popularity in terms of digital advancement.

[1] See https://e-estonia.com, last accessed on 25 May 2020.

Estonia is popularly claimed to use blockchain technology to secure e-voting (Jun, 2018) and to provide "the ability to 100% trust government data in any situation" (PWC, 2019, p. 7). This contributed to increasing the debate on how blockchain's potentialities regarding transparency and data ownership, among others, can be claimed at the institutional level as key to fostering more participatory approaches toward governance and returning the control of the data to the citizens. Through the inclusion of blockchain technologies in its digital architecture, the Estonian government claims to have fuelled these promises: by trusting the immutability and the decentralized nature of blockchain, citizens can be sure their information remains safe and therefore trust the government.

However, questioning how and to what extent Estonia is making use of blockchain is essential. Although E-Estonia is commonly referred to as the greatest example of a blockchain-based governmental project, little research has explored in-depth the ways in which blockchain is actually embedded into the digital infrastructure with a critical lens. Providing a detailed technical analysis of the uses of blockchain in Estonia is out of the scope of this article, yet by looking at the aforementioned applications of blockchain at an institutional level, we identified the existence of conflictual narratives regarding the Estonian use of blockchain inside the cryptocommunity. In other words, the case of Estonia becomes a relevant case study to research the interpretative flexibility of blockchain. This leads us to discuss to what extent institutional blockchains relate to the original blockchain promises of disruption and the crypto-imaginary, and how blockchain narratives may serve, instead, to foster institutional narratives that are beneficial for governmental political agendas.

To do so, first, it is necessary to briefly analyze the variety of political interpretations that subtend blockchain implementation, already mentioned in Section 2. By doing so, it will be possible to uncover a certain ambiguity revolving around the political significance of this "disruptive" technology and highlight its consequences for the blockchain public debate.

Blockchain narratives

Since e-Estonia is claimed to be one of the most advanced examples of blockchain use at a governmental level, its existence as a blockchain social application that goes beyond finance deserves further attention. The understanding of blockchain as a socio-technical object opens it indeed to several political interpretations regarding the potential of its affordances when applied to the social sphere.

To simplify the extensive spectrum of blockchain's political approaches, we are relying on Husain's research on blockchain imaginaries (2020). Although, as any other approach, it presents limitations concerning a highly individualized myriad of perspectives on blockchain technologies (Semenzin, 2021). Husain's categorization is useful to understand how blockchain narratives can be shaped according to different political agendas. In this sense, blockchain imaginaries can be clustered into two main groups: crypto-anarchists and crypto-institutionalists (Husain, 2020). The former refers to projects and initiatives that consider the disruptive potential of blockchain as a means to diminish the power of governmental institutions (e.g., Atzori, 2015; Husain, 2020). In contrast, the latter denotes an interest in government-led blockchain projects. In this sense, blockchain projects become polarized (Allen, 2017, p. 4) between those who aim at creating alternative systems of governance (crypto-anarchists) and those who aim at reinforcing existing institutional structures (crypto-institutionalists). This polarization leads to different narratives around blockchain, which compete for its hegemony in the discourse. In this sense, blockchain should be considered first and foremost a narrative technology (Reijers & Coeckelbergh, 2016) due to its capacity to shape people's understanding of the social world.

A relevant example of the dispute can be observed in the architecture that underlies blockchain. Although it is generally agreed that blockchain relies on a distributed architecture, there is a lack of consensus concerning a commonly accepted definition of which technical characteristics constitute a "real" blockchain. The conceptual distinction (Chowdhury et al., 2019, 167,932) between permissionless (public) and permissioned (private) blockchains was initially made by Tapscott and Tapscott (2016), arguing that both architectures can be considered blockchains. Permissionless blockchains can be seen as open networks in which anyone can participate. Individuals are fully autonomous and can act independently to send and receive information. In contrast, permissioned blockchains are closed networks: the addition and modification of data require administration permissions. Furthermore, in permissioned blockchains, it is possible to keep parts of the data transparent to some nodes while

keeping the rest hidden. To exemplify this distinction: the most popular blockchains, such as Bitcoin or Ethereum, are public blockchains, whereas Hyperledger is the best-known example of private blockchains.

Nevertheless, since blockchain was originally described as a decentralized ledger technology, other authors, such as Drescher (2017), argue that blockchains are exclusively related to open digital architectures since openness is a key characteristic to ensure the integrity of distributed systems. In this sense, the nature of blockchain remains vague: experts are still debating the fundamental requirements that have to be met to be considered "a blockchain" (Valiente & Tschorsch, 2021). In this regard, the case of Estonia becomes a valuable research object to observe such struggles for hegemony. Next, we discuss the methodological approach employed to analyze how blockchain operates as a contested socio-technical object in Estonia, exploring its significance through the lens of this conceptual debate.

Methodological approach and data collection methods

This study employed a multi-modal ethnographic approach to explore the socio-technical imaginaries (Jasanoff & Kim, 2015) that underpin blockchain as a social and cultural object in its applications beyond the financial sector. The data collection methods included participant observation, semistructured interviews, and documentary analysis. The first author collected and analyzed the data drawing on an ethnographic content analysis approach (Altheide, 1987) supported by the Computer-Assisted Qualitative Data Analysis Software NVivo 12.

Participant observation

The first author conducted participant observation throughout 1 month (September 2019) in Tallin (Estonia). She engaged in various online and offline activities, such as blockchain formal and informal meetings mostly organized in coworking, academic, and institutional spaces (e.g., the e-Estonia Briefing Center). She consistently created field notes. Participation was carried out to "follow the object", allowing the first author to access and understand the meanings of such a variety of individualized imaginaries surrounding the blockchain.

Semistructured interviews

Seven interviews were conducted, aiding a deeper understanding of the socio-technical imaginaries surrounding blockchain at an institutional level in the case of Estonia. Table A.1 provides an overview of the characteristics of the interviewees, which include governmental actors, blockchain developers, and well-known cryptographers. They were selected following a snowball sampling. It was concluded that this was the most suitable approach since the context, particularly at the institutional level, required the first author to gain access via personal recommendations to ensure the participation of governmental actors.

Documentary analysis

Documentary analysis was carried out to review and evaluate documents to elicit the diverse meanings surrounding blockchain as a contested socio-technical object. In total, 15 documents were analyzed and coded. These include official documents provided by institutional Estonian informants, technical whitepapers, and posts in Estonian blockchain-related blogs and Facebook groups.

Ethical considerations

The first author followed the ethical principles described by the "Università degli Studi di Milano",[2] as well as the recommendations from the Association of Internet Researchers (Markham & Buchanan, 2012). To ensure the right to privacy, individuals were anonymized in field notes, and interviewees signed consent forms that allowed for the use of all materials gathered.

E-Estonia's technical contested objects

The available official documentation on e-Estonia (https://e-estonia.com) explains that it relies on three distinct digital systems, so-called "three technological pillars of the digital state": "e-ID", "X-Road", and "KSI Blockchain".

[2] See https://www.unimi.it/it/ateneo/normative/codice-etico, last accessed on 25 May 2020.

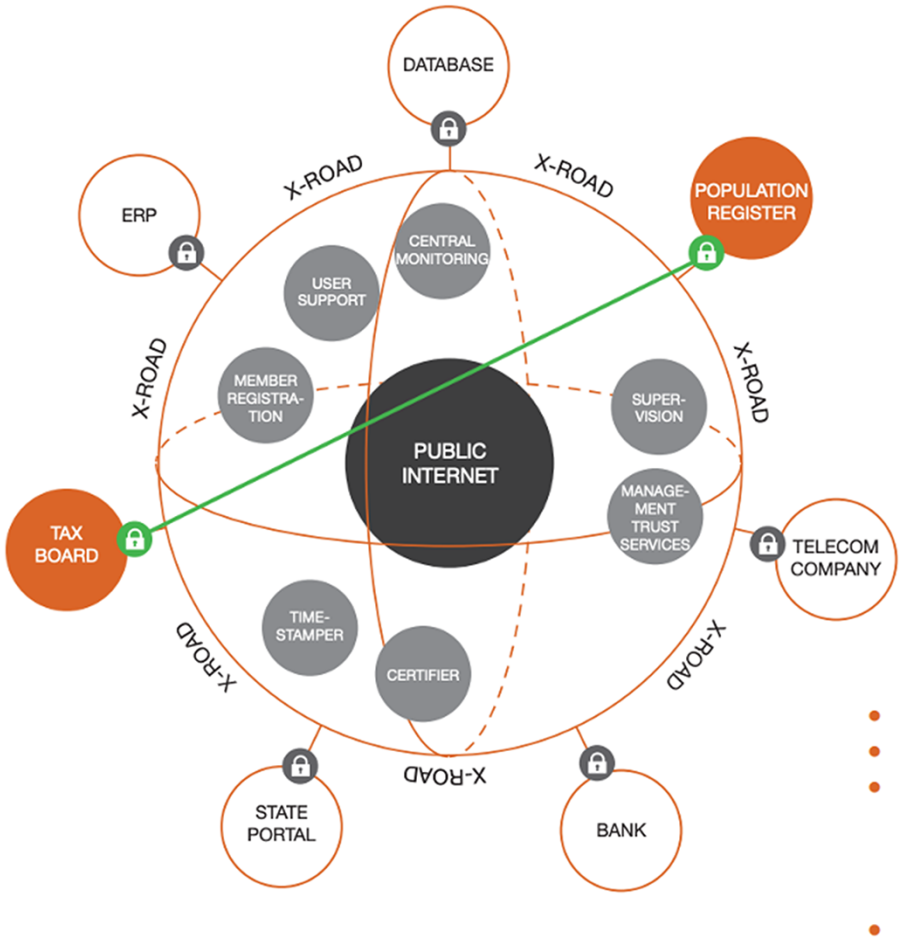

Figure 1. An overview of the functioning of X-Road as interoperability layer (PWC, 2019).

- "e-ID" refers to the electronic identity document, i.e., a **Digital Identity** service, which includes an electronic ID-card-based system used to access digital services.
- "X-Road" refers to an open-source **data exchange** layer solution that enables **interoperability** between institutional organizations (Kalvet, 2012b).
- "KSI Blockchain" allegedly refers to a timestamp system used for preserving the **integrity** of the digital documents within multiple public registries (e.g., healthcare, property).

In this section, we will explore the debates around these technologies, and in particular their consideration as blockchain-supported. The clashes of different narratives revolve around the contested "X-Road" and "KSI Blockchain" systems.

According to governmental sources, X-Road is "a decentralized technological and organizational environment enabling secure Internet-based data exchange between information systems. [..] [that] allowed Estonia to become a truly digital society" (PWC, 2019, p. 5). X-Road serves to exchange information between public institutions in a secure way and allows data to be automatically exchanged not only internally, but also between countries. In this regard, a connection of this kind has been implemented between Estonia and Finland (deploying its own X-Road) in 2017. Figure 1 shows an overview of how such digital architecture works.

As mentioned above, another component of the Estonian digital infrastructure comprises the so-called "KSI Blockchain" (KSI referring to Keyless Signature Infrastructure). Built by a company named Guardtime, "KSI Blockchain" is employed by NATO and the U.S. Department of Defense and used to

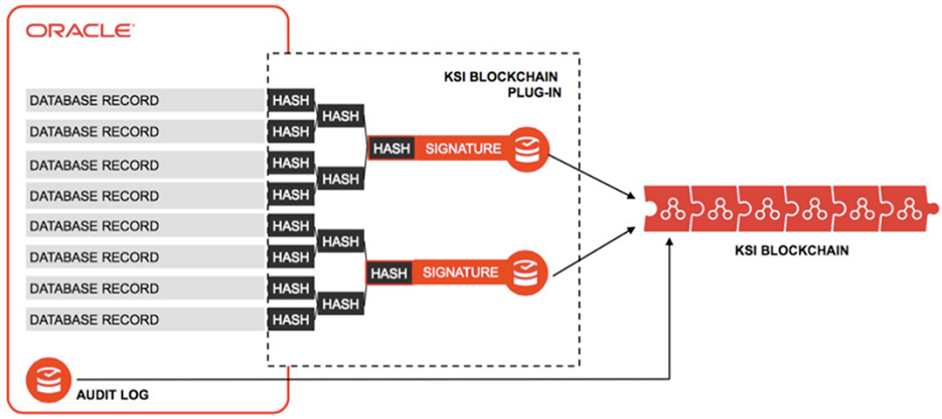

Figure 2. An overview of the functioning of the KSI blockchain (source: Guardtime). Extracted from https://lina.network/how-has-estonia-applied-blockchain-technology-to-the-e-government-system/, last accessed on 24 January 2022.

"guarantee the integrity and security of registries, identities, transactions and data privacy of its users" (Interview with an employee of Guardtime, informant 5).

The research informants pertaining to the governmental sphere blurred the distinctions between the functionality of the X-Road and the KSI Blockchain. In their words, "*the KSI blockchain can be seen just as a part of the X-Road system that helps to back the integrity of data*". Thus, according to them, X-Road includes the KSI Blockchain, and thus X-Road may be coined as a blockchain-supported system. This is supported by some official documents, presentations and media articles (Heller, 2017). However, there is still a lack of agreement about whether X-Road is actually based on a blockchain: the Nordic Institute for Interoperability Solutions (NIIS), for example, published a series of articles that criticized this position, arguing that X-Road does not rely on a blockchain or any distributed ledger for its operations (Kivimäki, 2018, 2021). This falls within this debate that we position our analysis: different interpretations of what affordances do make a "real" blockchain will help to shed light on different political approaches to this technology and its "disruptive" capabilities.

From our approach, it seems clear X-Road is independent of any distributed ledger operations, including KSI Blockchain. Still, it seems the E-Estonia infrastructure does use this KSI Blockchain for the timestamp of documents. Still, it immediately becomes clear that the country's digital architecture does not rely on a whole blockchain-based system. By discussing with a research participant from the Guardtime, it was in fact possible to discover that the Estonian registries secured by the KSI blockchain are limited to healthcare, property, business, and succession registries, as well as the digital court system and the State Gazette.

Figure 2 shows how KSI Blockchain operates. In basic terms, from each document, a "hash" is extracted, i.e., a unique sequence of codified characters that represent exactly that document. If the document is ever changed, its hash would change, and thus if a document is tampered it would be easily detected. The hash signatures are recorded in the "KSI Blockchain", a sequence of those hashes.

Another debate opens, although: is this KSI Blockchain an actual blockchain? In the academic literature referencing it, it is considered an example of blockchain or as a permissioned distributed ledger technology (e.g., Agarwal et al., 2021; Calvaresi et al., 2018; Hemalatha et al., 2021; Kuperberg et al., 2019; Nagasubramanian et al., 2020). When discussing the issue with Estonian informants, they reflected this debate by presenting significant opposite visions regarding blockchain use in Estonia. Some informants belonging to the crypto-anarchist sphere believed that the Estonian government was simply "using the hype of blockchain" and argued that E-Estonia should not be conceptualized as supported by blockchains (Kivimäki, 2018, 2021). An excerpt of an interview with a cryptographer from Tallinn explains this position:

> *"Almost nothing has been done in Estonia with blockchain. Yes, there are protected logs and there is a data structure, but it's not blockchain in terms of cryptocurrencies. It's not the blockchain that common people say it is a blockchain (sic)".* (Informant 1)

However, this position was definitely not shared among the crypto-institutionalist realm. On the contrary, informants from this sphere insisted on the idea that Estonia was an example to the World on how blockchain can serve the socio-political dimension. In the words of a relevant member of the Ministry of Economic Affairs and Communications: "*whatever has been done in Estonia with blockchain is a sort of telling everybody that's not just hype*" (Informant 3).

Interestingly, participants from the institutional sphere even claimed that Estonia was using blockchain long before Bitcoin appeared in 2008. These participants indeed agreed that the Estonian government was making use of blockchain and, furthermore, they argued that blockchain had actually been invented in Estonia. The argument was built upon the long tradition of cryptography in the country, which includes contributions such as the synchronization mechanisms employed to replicate databases in P2P networks. The following excerpt, from an interview of the aforementioned interviewee, illustrates this idea:

> "*We started to use blockchain before blockchain was introduced to the World by Satoshi Nakamoto's whitepaper. We just called it differently. We later knew we were doing that blockchain cool thing. I'm referring to the massive and scalable data integrity proof. This is how Estonia became the first blockchain power. We started to test this technology in 2008 and it went to production in 2012. We built an infrastructure platform*". (Informant 3)

This disagreement by the informants on whether the Estonian government does indeed use blockchain technologies led us to question what affordances would then constitute a "real" blockchain. Next, we explore this blockchain dispute in greater depth, exploring a key affordance: decentralization.

Decentralizing what? When blockchain's perspectives clash

Most literature regarding blockchain highlights that its main characteristic is that it relies on a distributed ledger, connecting it with the notion of decentralization. As a result, there is an emerging interest in exploring distributed ledger technologies as an alternative to the growing platformization of social interactions supported by centralized infrastructure (Srnicek, 2016). However, as argued by Vergne (2020, p. 2) decentralization has also become "a corporate cool factor associated with innovativeness or nimbleness; in this sense, it remains unclear what decentralization really entails as a design feature of organizations".

What does "decentralization" mean in the context of the use of blockchain-based technologies for the institutions of Estonia? Most informants explained that the blockchain systems employed at a governmental level in Estonia rely on private permissioned blockchains, which were developed by a commercial company. In this sense, Estonia makes use of a "closed" blockchain which reflects a centralized approach to the distributed ledger technology. According to the governmental informants, the choice of a private blockchain is mainly due to the possibility of "controlling" the flux of data. For example, Informant 20 explained:

> *"We don't use a public blockchain, because we still control who are those that send us data. We rely on a centralized, controlled system, also called a private, permissioned blockchain"* (Informant 4)

Other motivations often presented for using a private blockchain were that it is faster, safer, and more efficient since the network is managed by a handful of "trusted nodes that help the chain to remain unbiased" (informant 4). The sense of this position was better explained by an interviewee from the e-Estonia briefing Center, an official organism dedicated to the presentation of the e-Estonia project:

> "*Well, yes, decentralization of blockchain, of information on the blockchain is probably an advantage. It's just a question of how to govern it, right? I mean, if decentralization means in the end, you don't know where your data is anymore, then you have a problem, particularly if you're talking about the administration, right? So in that sense, why build a system where data sets themselves are distributed when you can just create an infrastructure where the holders of data store data on their premises and, if necessary, share this data with another agency that actually needs this data, right?"* (Informant 4)

These perspectives strongly clash with those from the crypto-anarchists, for whom blockchains are "unbiased" thanks precisely to the transparency provided by the openness of the ledgers (informant 2).

Furthermore, some interviewees deny the consideration of blockchain in the applications built by the Estonian government, a position which was also sustained by the already mentioned NIIS, which argued that since X-Road ecosystem is built around a centralized governance model managed by the X-Road operator, it cannot be considered a blockchain (Kivimäki, 2018). In this context, an informant who defined himself as a convinced "anarcho-capitalist", strongly criticized the "appropriation" of the word "blockchain" by the Estonian government:

> *"In Estonia there is no blockchain. X-Road is a scam. They are lying, I tell you! They started lying saying 'we have the blockchain, we are fully on the blockchain', which is non-sense. When they saw the power of blockchain technology, they thought 'we have to cook up some story and do some propaganda articles saying that we are already on the blockchain"* (Informant 2)

These differences in what a blockchain is are also tied to opposite political purposes and the perception of decentralization. Crypto-anarchist and libertarian blockchainers perceive decentralization as a means to restore the Internet to a free-flowing and open market of ideas and information. Thus, their narratives envision blockchain as a solution to social problems (Dodd, 2018; Karlstrøm, 2014). These social problems usually concern the existence of "repressive" governmental and financial actors that maintain power and control on citizens, limiting their freedom of action, as the same informant continued:

> *"You know, this Estonian X-Road system they are very proud about? It's very dangerous. It's very insecure! As long as the government likes you, it's cool. But if they don't like you anymore, they can partially switch you off. If you live in a country like Estonia and they push you out, you can literally go hunting in the forest. You can't do nothing (sic). Have you read the Republic of Plato? It's about how every nation gets corrupted. Now they are still being nice, but once you understand Estonia better you will understand that's just not true and that they just want to adopt a social credit system."* (Informant 2)

According to libertarian positions, talking about a "private blockchain" is nonsense because it may entail using ledgers and encryption. Still, private blockchains do not equate to the whole structure of the blockchain. Interestingly, not only libertarians criticized the institutional appropriation of the definition of blockchain, but even a couple of informants from the Estonian project disagreed, as exemplified by the words of an interviewee at the head of the Estonia e-Health project:

> *"We don't call it a blockchain, we call it a hash-chain. Because blockchain in its nature has no central controlled environment; but in Estonia there is always a responsible body which stores these hashes or timestamps. And in the healthcare context and E-government context, this is important".* (Informant 6)

The lack of a definitional agreement on private and public blockchains is relevant as it shows how political projects influence how this technology is explained and used. Institutional projects such as e-Estonia have nothing to do with the "real" blockchain to some actors. This has resulted in a clash of opposite political views and conflicting understandings of the meaning of decentralization. What arises from this clash of views is that, for some institutional and private actors, the blockchain should be permissioned because it enhances efficiency and speed. In contrast, those from more libertarian views argue that it is impossible to separate the essence of blockchain from a completely distributed and open architecture.

Overall, as the informant from the e-Health project stated, it perhaps seems that blockchain is indeed being used to re-centralize power in Estonia, rather than for decentralization:

> *"We are just using the blockchain data structures to inform— to make the existing institutions stronger".* (Informant 6)

This in-depth evaluation of how Estonian actors define the use of blockchain reveals how decentralization operates as a rhetorical strategy (Schneider, 2019). Concepts, such as blockchain and decentralization, change according to different political agendas. In other words, the lack of solid definitions leads to fluctuations in the concepts between different—sometimes radically opposite—visions of the world.

Can blockchain help strengthen traditional institutions rather than "debilitate" them, as originally envisioned? To tackle this issue, we will now further explore the reasons why blockchain is being implemented in Estonia.

Conceptualizing transparency at an institutional level

The lack of a universal agreement on how a blockchain should be designed also entails an important debate on the purposes for using blockchain and their relation to the concepts of privacy and data ownership.

Abundant literature discusses blockchain as a means to increase citizens' privacy (Tapscott & Tapscott, 2016; Zyskind & Nathan, 2015), arguing that the use of encryption is key to increasing participants' privacy. Privacy on the Internet is typically conceptualized as a right to maintain a private space that is free from external interference (Nissenbaum, 2009). Privacy, in this sense, is often tied to the discussion on the accumulation of power on the Internet, i.e., surveillance capitalism (Zuboff, 2015), as well as the debate on citizens' data ownership.

The lack of a universal agreement on how a blockchain should be designed also leads to an important debate on the purposes for using blockchain and their relation to the concepts of privacy and data ownership. We identified a similar lack of agreement on which kind of privacy would be enhanced by blockchain. As in the previous case, the issue originates from the permissioned vs. public blockchain debate. While blockchain literature seems to tie this concept to the idea of encryption and anonymity, supporters of public blockchains place more attention on the concepts of transparency and peer validation. Transparency, in this sense, clashes with the classical concept of privacy because, on a public blockchain, everybody can see others' transactions. To clarify this, an informant from Tallinn with a long history of building encrypted systems explained how blockchain technologies could not be considered a tool for privacy:

> *"I don't see any common point between privacy and blockchain. It's completely the opposite. Blockchain makes things (data) public, not private. I think that those who talk about privacy and blockchain don't know what it is at all about."* (Informant 1)

In the crypto-community, particularly for crypto-institutionalists, transparency offers an affordance to increase trust toward governmental institutions, as discussed in Section 3. In the case of Estonia, however, an institutional research participant considered that this affordance remained "somehow invisible to citizens", as blockchain was not used to protect their data "from" the government. On the contrary, it is instead the "system administrators" in control of their data who benefit from it, as the following extract of the interview illustrates:

(Interviewer) *"So why do you think the blockchain is useful for citizens in Estonia?"*
(Informant 4) *"Well I think the citizen doesn't really know anything about it, and it doesn't make a big difference for the citizens, whether it's blockchain or whether it's some other technology. In general, I would say the benefit in the end is actually for the administrators of the systems They can understand whether somebody unauthorized has actually gotten access to data. Right? Because they can pretty much track every change to data with the help of this technology. So you can just prove afterwards that somebody changed—something happened to the data."*

The use of a permissioned blockchain exploits the concept of "transparency" in terms of controlling the chain history by those having the appropriate permissions, rather than employing blockchains as a means to increase governmental transparency. This governmental interpretation of transparency has its roots in the history of Estonia's sociopolitical context. The use of blockchain in Estonia is mainly related to the need for cybersecurity. Most participants highlighted how the transition toward a digital society implied a higher degree of exposure to cyberattacks. Notably, they frequently mentioned Estonia's complex relationship with Russia. After receiving a massive cyberattack in 2007, cybersecurity became a central issue and led to implementing blockchain at an architectural level. The excerpt below, from an interview with an informant from the e-Estonia Briefing Center, illustrates these views:

> *"The only reason why we're using KSI Blockchain today is that we needed to find a way, in the aftermath of the cyber attacks in 2007, of how to impenetrability prove (sic) that somebody has actually taken access and changed data, so that you, afterwards—so that your system administrators could actually take action. This is often the problem*

with cyber attacks, etcetera, that the attackers are in the system for way too long before they are discovered. So with this kind of technology where changes to data are being recorded, with the help of these hashes, you can react much faster and take action. So the only reason back then was that we needed a tool that would allow us to make conclusions about whether an access was authorized or not. And then the tool was found. It was not like the tool was there before. And then we try to find out how to use the tool, right? So it's actually the organizational need that triggered the use of this technology." (Informant 3)

In sum, the use of blockchain in Estonia is mainly driven by political priorities concerning the necessity for building resilient infrastructures that could avoid further external intrusions. This application results in a downplaying of the relevance of citizens' privacy in terms of mass surveillance and commercial use of personal data. In this sense, the promises of increasing governmental trust through blockchain reside primarily in the institutional capacity to defend citizens' data against foreign attacks and maintain the digital architecture intact. Despite the initial promises, blockchain does not address any major societal issue like institutional trust or corruption. Instead, in the case of E-Estonia, blockchain has become a vague and contested object, which centralized institutions employ to maintain control of digital data.

Discussion and concluding remarks

This article contributes to the literature on blockchain and governance by identifying blockchain as a contested socio-political object prone to contradictory political imaginaries regarding its potentialities. As we have seen, at an institutional level, the most praised of blockchain's affordances (e.g., decentralization and transparency) become disputed, floating concepts.

Based on the affordances (Atzori, 2015; Gerard, 2017; O'Dwyer, 2015; Rozas, Tenorio-Fornés, Díaz-Molina, et al., 2021; Rozas, Tenorio-Fornés, Hassan, et al., 2021; Tapscott & Tapscott, 2016) mentioned above, blockchain is often discussed as a 'disruptive' technology that could reshape several political, economic, and social relations in the digital sphere. For this reason, blockchain has attracted attention from political institutions, which are interested in the use of distributed architectures to enhance 'bigger trust' toward governments and politicians. It is argued that the decentralized and transparent nature of blockchain facilitates citizens' control over governmental activities and provides solutions to problems of data misuse and corruption. Nevertheless, the crypto-anarchist origins of blockchain, more focused on disintermediation and the disappearance of traditional institutions, have also led to the emergence of a debate concerning blockchain's key concepts and their connection with these notions of 'disruption' and 'trust'. All of these differing political interpretations originate from ideological clashes, which should not be ignored. In this sense, the case of Estonia explored in this article reveals an essential difference in the appropriation of narratives surrounding blockchain's affordances.

Since blockchain's technical dimensions are contested, the narrative surrounding the technology reveals contrasting discourses originating from the distinction between open and closed blockchains. On the one hand, crypto-anarchists (Husain, 2020), the pioneers of blockchain and cryptocurrencies, believe that a distributed ledger can be a blockchain exclusively if it is global and open. According to these views, only open and decentralized architectures reflect the fundamental nature of the technology and thus can be considered 'real' blockchains. On the other hand, crypto-institutionalists (Husain, 2020) see closed blockchains as tools to build more resilient digital architectures that can help governments exert more control over their informational data fluxes. According to them, permissioned blockchains are more effective and safer while maintaining decentralized ledgers. The case of Estonia provides empirical evidence of this lack of agreement regarding blockchain definitions. We identified significantly opposite understandings of fundamental concepts such as decentralization, transparency, and trust. Overall, this led some blockchain enthusiasts to argue that Estonia does not indeed use blockchain and that, on the contrary, blockchain appropriation is part of creating governmental propaganda for gaining worldwide visibility. In fact, although according to different sources decentralized technologies in Estonia were deployed for security and administrative reasons in the first place, the narrative around blockchain and DLTs seem to have been later adopted to ride the wave of the 'hype'. In this sense, the distinction between crypto-anarchist and crypto-institutionalists we drew on (Husain, 2020) is a useful lens to understand the hegemonic aspirations that underlie blockchain implementations. Through this lens, we show how in the institutional context of this case study blockchain is, above all, a powerful concept to be exploited in the public imagination according to different political agendas.

Moreover, the data collected for this study reveal how blockchain applications at a governmental level have been employed to reinforce already existing centralized practices. Thus, at least in the case of Estonia, blockchain technologies applied at the public and institutional level appear to be detached from the promise of societal disruption, yet still exploit blockchain's "rhetoric of empowering the disenfranchised through decentralized decision-making process, enabling anonymous of transactions, dehumanizing trust" (Gikay & Stanescu, 2019). In Estonia, the concept of transparency is employed as a synonym of data privacy, in which the governmental trust would arise from warranting cybersecurity and control over data. Additionally, the concept of decentralization remains in the background to provide an illusion of disruption. These conceptualizations clash with the original promises of crypto-anarchist blockchain enthusiasts and provide an ambiguous picture of the meaning of blockchain in governance. Further research could investigate similar clashes within the aforementioned narratives in other uses of blockchain at an institutional level.

In conclusion, due to the lack of universal definitions of what constitutes a blockchain, different technological narratives are emerging surrounding a concept that offers influential areas for its exploitation in the public imaginaries, according to different political agendas. What is ultimately at stake within this struggle is who obtains the power to define what is deemed a "real" blockchain and hegemonize the concept to serve their purposes.

Supplementary material

Supplementary material is available online at *Policy and Society* (http://mtp.oxfordjournals.org/).

Acknowledgements

We would like to thank Alessandro Gandini, Paola Rebughini, Anu Masso and David DueñasCid for their valuable comments, as well as Tabitha Whittall for her help in copyediting and proofreading this article. Finally, we would like to thank Alexandra Elbakyan (Sci-Hub) for her contribution to making scientific knowledge available to everyone.

Funding

This work was partially supported by the project P2P Models (https://p2pmodels.eu) funded by the European Research Council ERC-2017-STG (grant no.: 759207) and by the project Chain Community funded by the Spanish Ministry of Science, Innovation and Universities (grant no.: RTI2018-096820-A-100).

Conflict of interest

None declared.

References

Agarwal, A. K., Tiwari, R. G., Kaushal, R. K., & Kumar, N. (2021). A systematic analysis of applications of blockchain in healthcare. In *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)*. IEEE, Waknaghat, India.

Ainsworth, R. T., & Shact, A. (2016). Blockchain (distributed ledger technology) solves VAT fraud. *SSRN Electronic Journal*, 16–41.

Alexopoulos, C., Charalabidis, Y., Loutsaris, M. A., & Lachana, Z. (2021). How blockchain technology changes government. *International Journal of Public Administration in the Digital Age*, *8*(1), 1–20. https://doi.org/10.4018/IJPADA.20210101.oa10.

Allen, D. W. E. (2017). *Discovering and developing the blockchain cryptoeconomy* (ID 2815255). Social Science Research Network. https://papers.ssrn.com/abstract=2815255.

Altheide, D. L. (1987). Reflections: Ethnographic content analysis. *Qualitative Sociology*, *10*(1), 65–77. https://doi.org/10.1007/BF00988269.

Antonopoulos. (2014). *Bitcoin security model: Trust by computation*. O'Reilly- Radar. 2014. http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html.

Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary? *SSRN Electronic Journal*.

Atzori, M., & Ulieru, M. (2017). *Architecting the eSociety on blockchain: A provocation to human nature* (ID 2999715). Social Science Research Network. https://papers.ssrn.com/abstract=2999715.

Cagigas, D., Clifton, J., Diaz-Fuentes, D., & Marcos, F.-G. (2021). Blockchain for public services: A systematic literature review. *IEEE Access*, *9*, 13904–13921. https://doi.org/10.1109/ACCESS.2021.3052019.

Calvaresi, D., Dubovitskaya, A., Calbimonte, J. P., Taveter, K., & Schumacher, M. (2018). Multi-agent systems and blockchain: Results from a systematic literature review. In: Demazeau, Y., An, B., Bajo, J., Fernández-Caballero, A. (Eds.), *Advances in Practical Applications of Agents, Multi-Agent Systems, and Complexity: The PAAMS Collection*. vol 10978 (pp. 110–126). Springer International Publishing. Lecture Notes in Computer Science. https://doi.org/10.1007/978-3-319-94580-4_9.

Catlow, R. (2017). *Artists re: Thinking the blockchain*. Torque Editions & Furtherfield. https://doi.org/10.1109/ACCESS.2019.2953729.

Chowdhury, M., Jabed Morshed, M. D., Ferdous, S., Biswas, K., Niaz Chowdhury, A. S. M., Kayes, M. A., & Watters, P. (2019). A comparative analysis of distributed ledger technology platforms. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 167930–167943. https://doi.org/10.1109/ACCESS.2019.2953729.

Christensen, C. M. (2006). The ongoing process of building a theory of disruption. *The Journal of Product Innovation Management*, *23*(1), 39–55. https://doi.org/10.1111/j.1540-5885.2005.00180.x.

Cila, N., Ferri, G., Martijn, D. W., Gloerich, I., & Karpinski, T. (2020). The blockchain and the commons: Dilemmas in the design of local platforms. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–14. CHI'20. Association for Computing Machinery, New York, NY, USA.

De Filippi, P., & Loveluck, B. (2016). *The invisible politics of bitcoin: Governance crisis of a decentralized infrastructure*. https://papers.ssrn.com/abstract=2852691.

Dodd, N. (2018). The social life of bitcoin. *Theory, Culture & Society*, *35*(3), 35–56. https://doi.org/10.1177/0263276417746464.

Drescher, D. (2017). *Blockchain basics: A non-technical introduction in 25 steps. PDF* (1st ed.). APress.

Faqir-Rhazoui, Y., Arroyo, J., & Hassan, S. (2021). A comparative analysis of the platforms for decentralized autonomous organizations in the ethereum blockchain. *Journal of Internet Services and Applications*, *12*(1), 1–20.

Filippi, P. D., & Hassan, S. (2016). Blockchain technology as a regulatory technology: From code is law to law is code. *First Monday*, *21*, 12.

Fritsch, F., Emmett, J., Friedman, E., Kranjc, R., Manski, S., Zargham, M., & Bauwens, M. (2021). Challenges and approaches to scaling the global commons. *Frontiers in Blockchain*, *4*(578721), 9. https://doi.org/10.3389/fbloc.2021.578721.

Galen, D., Brand, N., & Boucherle, L. (2018). *Blockchain for social impact: Moving beyond the hype*. Standford University. https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/study-blockchain-impact-moving-beyond-hype.pdf.

Galend, D., Brand, N., & Boucherle, L. (2018). *Blockchain for social impact: Moving beyond the hype*. https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/study-blockchain-impact-moving-beyond-hype_0.pdf.

Gerard, D. (2017). *Attack of the 50 foot blockchain: Bitcoin, blockchain, ethereum & smart contracts*. David Gerard.

Gikay, A. A., & Stanescu, C. G. (2019). Technological populism and its archetypes: Blockchain and cryptocurrencies. *SSRN Electronic Journal*, (2), 66–109.

Golumbia, D. (2016). *The politics of bitcoin: Software as right-wing extremism*. U of Minnesota Press.

Hassan, S. J., Brekke, K., Atzori, M., Bodo Balatz, K., Beecroft, D. R., Orgáz-Alonso, C., Vicente-Martínez, E., López-Morales, G., & Figueras-Aguilar, A. (2020). *Scanning the European Ecosystem of Distributed Ledger Technologies for Social and Public Good*. In: Roque Mendes Polvora, A., Hakami, A. and Bol, E. (Eds.), EUR 30364 EN, Publications Office of the European Union, Luxembourg. https://doi.org/10.2760/802653.

Hayes, A. (2016). Decentralized banking: Monetary technocracy in the digital age. In P. Tasca, T. Aste, L. Pelizzon & N. Perony (Eds.), *Banking beyond banks and money* (pp. 121–131). Springer International Publishing.

Heller, N. (2017, December 11). Estonia, the digital republic. *The New Yorker*. https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic.

Hemalatha, P., Balaji, S., Chandru, E., & Pelleti-Pradeep Kumard, S. D. (2021). Monitoring and securing the healthcare data harnessing IOT and blockchain technology. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(2), 2554–2561. https://doi.org/10.17762/turcomat.v12i2.2213.

Heuermann, C. (2015). *Governance 2.0: A Hayekian approach to (r)evolutionary self-governance by cryptocurrencies*. University of Konstanz.

Hileman, G., & Rauchs, M. (2017). Global cryptocurrency benchmarking study. *Cambridge Centre for Alternative Finance*, 33, 33–113. https://econpapers.repec.org/RePEc:jbs:altfin:201704-gcbs.

Huckle, S., & White, M. (2016). Socialism and the blockchain. *Future Internet*, *8*(4), 49. https://doi.org/10.3390/fi8040049.

Husain, S. O. (2020). *(De)coding a technopolity: Tethering the civic blockchain to political transformation* [PhD]. Wageningen University.

Jasanoff, S., & Kim, S.-H. (2015). *Dreamscapes of modernity: Sociotechnical imaginaries and the fabrication of power*. University of Chicago Press.

Johnston, D. A. (2014, August 30). *Everything will be decentralized*. Medium. Medium. https://medium.com/@DJohnstonEC/everything-will-be-decentralized-d7dcedca45e.

Jun, M. (2018). Blockchain government - a next form of infrastructure for the twenty-first century. *Journal of Open Innovation: Technology, Market, and Complexity*, 4(1).

Kalvet, T. (2012a). Innovation: A Factor Explaining E-Government Success in Estonia. *Electronic Government, an International Journal*, 9(2), 142.

Kalvet, T. (2012b). Innovation: A factor explaining E-government success in Estonia. *Electronic Government, an International Journal*, 9(2), 142.

Karlstrøm, H. (2014). Do libertarians dream of electric coins? The material embeddedness of bitcoin. *Distinktion: Journal of Social Theory*, *15*(1), 23–36.

Kivimäki, P. (2018, April 26). *Nordic institute for interoperability solutions — there is no blockchain technology in X-road*. Nordic Institute for Interoperability Solutions. https://www.niis.org/blog/2018/4/26/there-is-no-blockchain-technology-in-the-x-road.

Kivimäki, P. (2021, October 12). *Nordic institute for interoperability solutions — there's no distributed ledger technology (DLT) in X-road." Nordic institute for interoperability solutions*. https://www.niis.org/blog/2021/10/3/theres-no-distributed-ledger-technology-dlt-in-x-road.

Kuo, T.-T., Rojas, H. Z., & Ohno-Machado, L. (2019). Comparison of blockchain platforms: A systematic review and healthcare examples. *Journal of the American Medical Informatics Association: JAMIA*, *26*(5), 462–478. https://doi.org/10.1093/jamia/ocy185.

Kuperberg, M., Kemper, S., & Durak, C. (2019). Blockchain usage for government-issued electronic IDs: A survey. In: Proper, H., Stirna, J. (Eds.), *Advanced Information Systems Engineering Workshops*. CAiSE 2019. vol 349 (pp. 155–167). Springer International Publishing. Lecture Notes in Business Information Processing. https://doi.org/10.1007/978-3-030-20948-3_14.

Macdonald, M., Liu-Thorrold, L., & Julien, R. (2017). *The blockchain: A comparison of platforms and their uses beyond bitcoin*. Working Paper.

Markham, A., & Buchanan, E. (2012). *Ethical decision-making and internet research*. Association of Internet Researchers. http://aoir.org/reports/ethics2.pdf.

May, T. (1988). *The crypto anarchist manifesto*. https://www.activism.net/cypherpunk/crypto-anarchy.html.

Nagasubramanian, G., Sakthivel, R. K., Rizwan Patan, A. H., Gandomi, M. S., & Balusamy, B. (2020). Securing E-health records using keyless signature infrastructure blockchain technology in the cloud. *Neural Computing & Applications*, *32*(3), 639–647. https://doi.org/10.1007/s00521-018-3915-1.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. http://bitcoin.org/bitcoin.pdf.

Nguyen, Q. K. (2016). Blockchain - A Financial Technology for Future Sustainable Development - IEEE Conference Publication, Taipei, Taiwan.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books.

Novak, M. (2019). Crypto-friendliness: Understanding blockchain public policy. *Journal of Entrepreneurship and Public Policy*, 9(2), 165–184. https://doi.org/10.1108/JEPP-03-2019-0014.

O'Dwyer, R. (2015). *The revolution will (not) be decentralised: Blockchains*. http://commonstransition.org/the-revolution-will-not-be-decentralised-blockchains/.

Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science*, *14*(3), 399–441. https://doi.org/10.1177/030631284014003004.

Pólvora, A., Nascimento, S., Lourenço, J., & Scapolo, F. (2020). Blockchain for industrial transformations: A forward-looking approach with multi-stakeholder engagement for policy advice. *Technological Forecasting and Social Change*, 157(August), 120091. https://doi.org/10.1016/j.techfore.2020.120091.

PWC. (2019). *Estonia - the digital republic secured by blockchain*. https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf.

Reijers, W., & Coeckelbergh, M. (2016). The blockchain as a narrative technology: Investigating the social ontology and normative configurations of cryptocurrencies. *Philosophy & Technology*, 31(1), 103–30.

Risius, M., & Spohrer, K. (2017). A blockchain research framework: What we (don't) know, where we go from here, and how we will get there. *Business & Information Systems Engineering*, 59(6), 385–409. https://doi.org/10.1007/s12599-017-0506-0.

Rozas, D., Tenorio-Fornés, A., Díaz-Molina, S., & Hassan, S. (2021). When ostrom meets blockchain: Exploring the potentials of blockchain for commons governance. *Sage Open*, *11*(1), 1–14. https://doi.org/10.1177/21582440211002526.

Rozas, D., Tenorio-Fornés, A., & Hassan, S. (2021). Analysis of the potentials of blockchain for the governance of global digital commons. *Frontiers in Blockchain*, 4(577680), 1–13. https://doi.org/10.3389/fbloc.2021.577680.

Schäfer, M. T., & Van Es, K. (2017). *The datafied society: Studying culture through data*. Amsterdam University Press. https://doi.org/10.5117/9789462981362.

Schneider, N. (2019). Decentralization: An incomplete ambition. *Journal of Cultural Economy*, *12*(4), 265–285. https://doi.org/10.1080/17530350.2019.1589553.

Semenzin, S. (2021). Blockchain & data justice. The political culture of technology. *University of Milan*.

Srnicek, N. (2016). *Platform capitalism*. Wiley.

Sullivan, C., & Burger, E. (2017). E-residency and blockchain. *Computer Law & Security Review*, 33(4), 470–481. https://doi.org/10.1016/j.clsr.2017.03.016.

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly.

Tammpuu, P., & Masso, A. (2019). Transnational digital identity as an instrument for global digital citizenship: The case of Estonia's E-residency. *Information Systems Frontiers*, *21*(3), 621–634. https://doi.org/10.1007/s10796-019-09908-y.

Tan, L., Tivey, D., Kopunic, H., Babidge, W., Langley, S., & Maddern, G. (2020). Part 2: Blockchain technology in health care. *ANZ Journal of Surgery*, 90(12), 2415–2419.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin.

Valiente, M.-C., & Tschorsch, F. (2021). Blockchain-based technologies. *Internet Policy Review*, *10*(2), 1–6. https://policyreview.info/pdf/policyreview-2021-2-1552.pdf.

Vergne, J. P. (2020). Decentralized vs. Distributed organization: Blockchain, machine learning and the future of the digital platform. *Organization Theory*, *1*(4), 263178772097705. https://doi.org/10.1177/2631787720977052.

World Economic Forum. (2020). *Exploring blockchain technology for government transparency: Blockchain-based public procurement to reduce corruption*. https://www.google.com/url?q=http://www3.weforum.org/docs/WEF_Blockchain_Government_Transparency_Report.pdf&sa=D&source=editors&ust=1622023201515000&usg=AOvVaw3C0jF0bRubIOEHDYQhLAz4.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75–89.

Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. *2015 IEEE Security and Privacy Workshops*, 180–184.