CENTRE FOR TECHNOLOGY & GLOBAL AFFAIRS

www.ctga.ox.ac.uk

UNIVERSITY OF OXFORD

Working Paper Series – No. 7 December 2017

Blockchains for Governmental Services: Design Principles, Applications, and Case Studies

Ivan Martinovic
Associate Professor of Computer Science
University of Oxford
ivan.martinovic@cs.ox.ac.uk

Lucas Kello
Senior Lecturer in International Relations
Director of the Centre for Technology and Global Affairs
University of Oxford
lucas.kello@politics.ox.ac.uk

Ivo Sluganovic
DPhil Candidate in Computer Science
University of Oxford
ivo.sluganovic@cs.ox.ac.uk

European Union
European Social Fund

Investing
in your future

This publication is funded by the European Social Fund and the Estonian Government

1 INTRODUCTION

A blockchain is a technology for constructing specific types of distributed databases composed of immutable blocks of data, each containing a list of transactions and a unique reference to its predecessor block. Blockchain technology is the subject of intense and growing attention among governments, technology developers, and private investors. The British government, for example, has recognized that this technology "could transform the conduct of public and private sector organizations."[1] In Estonia, private firms are planning to use blockchain-related technology in conjunction with digital ID cards to conduct shareholder voting.[2] Researchers at the European Parliament have concluded that the new technology could deliver a "revolution in the security and transparency that is needed to enable e-voting."[3]

The most prominent contemporary applications of blockchain technology are cryptocurrencies, such as bitcoin.[4] The research and deployment of other practical applications remains limited, however. As one small survey of the literature indicates, less than 20 percent of existing academic publications on this technology focus on its applications.[5] This paper, consequently, will not focus on cryptocurrencies; rather, it uses bitcoin as an example to illustrate the basic underlying principles and properties that allow blockchains to function—the creation, distribution, and protection of distributed ledgers as well as the potential to ensure the integrity of sensitive data records.

In particular, the paper will discuss a case study of the Estonian government's integration of blockchains into its digital infrastructure to secure both public and internal governmental records.[6] The paper argues that the Estonian government's use of blockchains to support public services demonstrates the technology's many advantages. These advantages range from higher transparency to process efficiency to increased resilience against various cyberattacks. The paper also discusses the technology's potential application in other contexts and countries, such as in Britain, where blockchains are attracting increasing government attention and for which the Estonian experience offers potentially useful lessons.

Specifically, the objective of the paper is to explore two research questions. The first relates to the underlying technology: What are the technical rudiments of blockchain technology? The second question is of a more applied nature: What is the current state of blockchain integration in the protection of Estonian state records?

Finally, it is important to emphasize that many aspects of blockchain-based technologies are still undergoing research. One of the main challenges in introducing blockchain-based technologies is finding a balance between various, often conflicting system objectives, such as security versus performance and assurance versus control. As an example, despite the public nature of the original blockchain proposals, many so-called private, permissioned blockchains are currently being designed with the objective to keep the costs of running a blockchain low while still achieving specific design objectives. Given the large number of different shapes and forms, however, the security guarantees of such private blockchains are difficult to generalize because they depend on a concrete blockchain implementation.

2 A BRIEF INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

In 2008, bitcoin, the first widely used digital currency, was anonymously proposed in a whitepaper[7] that quickly grabbed the attention of several online communities. This was largely due to its proposing a functional prototype of a payment system in which consensus about the past transactions and the current states of assets could be efficiently and securely achieved among mutually untrusting participants without the need for any trusted intermediaries. Since the proposal was heavily based on core cryptographic principles, such as public-key cryptography and one-way functions (which we briefly review in later sections), bitcoin is considered to be the first widely used cryptocurrency. It is important to

The authors are grateful for the helpful insights and information that they received in technical interviews with Andres Kütt, Mikk Lellsaar, Ivo Lõhmus, and Kuldar Aas during the preparation of this paper.

1 "Beyond Block Chain" (London: Government Office for Science, 2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

2 See "Nasdaq's Blockchain Technology to Transform the Republic of Estonia E-Residency Shareholder Participation," Nasdaq Press Release, February 16, 2016, http://ir.nasdaq.com/releasedetail.cfm?releaseid=954654.

3 Philip Boucher, "What If Blockchain Technology Revolutionised Voting?" *What If…?* Scientific Foresight Unit (STOA), European Parliament Research Service, Brussels, September 2016, http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA%282016%29581918_EN.pdf.

4 Jerry Brito and Andrea Castillo, "Bitcoin: A Primer for Policymakers," Mercatus Center, George Mason University, Fairfax, Va., 2013, https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf.

5 See Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review." Plos One, October 2016.

6 See "Blockchain," https://e-estonia.com/tag/blockchain/; "Blockchain-Enabled Cloud: Estonian Government selects Ericsson, Apcera and Guardtime", August 2015, https://guardtime.com/blog/blockchain-enabled-cloud-estonian-government-selects-ericsson-apcera-and-guardtime.

7 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," www.bitcoin.org (2008). https://bitcoin.org/bitcoin.pdf.

emphasize, however, that while blockchain technology was first proposed and introduced in the context of the bitcoin cryptocurrency, its applications are significantly wider.

While bitcoin is a recent invention, the majority of underlying technology that enables it has existed for decades. From a security perspective, the technical challenges of designing a digital alternative to physical money are in many ways similar to the general security challenges behind standard cryptographic algorithms and security protocols. Therefore, the cryptographic components of the bitcoin system are based on well-understood and established cryptographic constructs. While the main components have been known before its introduction, though, it is the intricate and elegant combination of various concepts and ideas from disparate research fields, such as cryptography, networking and distributed systems, game theory, and economics, that make understanding and analysis of bitcoin and other applications of the blockchain technology a very challenging and active area of research and innovation.

The ensuing discussion introduces the main security objectives and cryptographic constructs that are used to achieve these objectives within realistic threat models.

2.1 Main Technical Concepts and System Properties

In the current section, we briefly introduce some of the technical concepts that are important for understanding blockchain technology.

Confidentiality is used to keep the content of information accessible only to individuals who are authorized to access it. The authorization can be established using an authentication credential (e.g., by proving the possession of a secret key). Within this context, *secrecy* is synonymous with confidentiality and privacy. There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms (also called ciphers), which render data unintelligible to casual observers. The most common way of achieving confidentiality is encryption, which entails the use of a cipher with an encryption key over data that needs to be protected. Only a person with the correct decryption key will be able to decrypt the data.

The ***integrity*** of information guarantees that an unauthorized party has not modified the information. Because data manipulation can be achieved by simple methods such as insertion, deletion, and substitution of information, the goal of integrity is to *detect* data manipulation and not to accept the manipulated data. This property can be achieved by applying different core cryptographic ideas (primitives), the most common of which are cryptographic *hash functions*. The cryptographic hash functions are security primitives that provide a compact representation of data (called *hash value*) while making it practically impossible for an attacker to change the data without changing the hash value. This is achieved if the hash function has two important properties that make it *cryptographically strong*: first, the hash values of different pieces of data are necessarily different (no hash collisions); and second, there is no way to extract the original data from its hash. A very simple example of applying a (weak) hash function to a numerical spreadsheet would be to multiply each numeric value in the spreadsheet with the index of its row and column. The sum of all such numbers could be considered a simple hash value of the whole spreadsheet: adding, removing, or changing any of the values in the spreadsheet is likely to change the total sum, while there is no way to reverse the hashing process by extracting the original data from the spreadsheet. Given that it is difficult to change the spreadsheet so that the hash remains the same, securely storing and retrieving only the hash value of the spreadsheet is sufficient to verify at any subsequent moment that no data has been changed.

Authentication can be subdivided into two major classes: *entity authentication* and *data origin (and provenance) verification*. Entity authentication is used by parties to identify each other when they begin communicating. Entity authentication protocols include a claim of identity and methods to verify the claim. Data origin (and provenance) verification operates in a similar fashion. Information delivered from communication should be authenticated as to origin, date of origin, data content, time sent, etc. This can be achieved with various cryptographic protocols, depending on the definition of the claimed identity. In the context of blockchain technology, authentication is an important aspect of the authorization process—that is, it enables permission to read from and write to blockchains, which is common in private (i.e., permissioned) blockchains. If anyone can join the network and write to the blockchain, the blockchain is considered *unpermissioned* or *public*. This means that no authority is required to grant permissions on reading from and writing to the blockchain. Such a blockchain is also called *immutable* as it is highly censorship resistant. The main complexity of public blockchains comes from the computational resources required to execute consensus mechanisms, which are used to prevent misbehaviour, detect attacks, and resolve conflicts resulting from blockchain inconsistencies.

Availability of information or services refers to ensuring that authorized entities are able to access the relevant data. Traditionally, availability has not been an objective of cryptographic primitives because it is more of a system-level property. That is, access to information depends on various factors, such as protocols, channel capacity, and other network-related properties. Any of these factors can affect the availability of services and information. Therefore, it is not only a security property but also one directly related to

the safety of systems. A conventional approach to improving the availability of a system is to increase the system's resources, for example, by introducing redundancy (such as "overprovisioning") of the critical system components.

In addition to these fundamental security objectives, blockchain systems are usually based on various ***Proofs-of-Work*** (PoW). The general and historic aim of PoW has been to protect service providers against resource-depletion attacks. Requesting a service usually requires some sort of non-negligible resource investment from the provider's side. For example, if a client wants to access a web page, it needs to establish a connection with a web server. To establish the connection, the server side must invest resources (such as computational power, storage, or bandwidth) to run the network protocol requested by the client and return the requested resources. If a client sends many such requests, however, the amount of work on the server's side could lead to "denial-of-service" (DoS) attacks, in which the targeted server is unable to process other clients' legitimate requests. It is difficult to detect whether a client is misbehaving in this way, though, because the requests can be manipulated so that they seem to come from different clients. The PoW concept tries to resolve this problem by requesting commitment (in terms of a resource investment) from the initiating side before the responding side starts investing resources in the communication.

In the context of blockchains, contributing to the blockchain deliberately requires significant resource investment. This is achieved by requiring that each new block added to the blockchain must necessarily have a particular, uniquely defined PoW attached to it, proving that significant investment of resources has been made. Most common blockchains require PoW in the form of a solution to so-called cryptographic puzzles, which involve searching for randomly distributed information over a large search space. This is a laborious task that, depending on the search space, takes predictable time to solve, and can only be sped up by parallelization of computing resources, which increases physical resource investment. In bitcoin's terminology this is called *mining*, and requires generating a correct block signature for the blockchain based on the specific requirements for a valid signature. Once PoW is created and submitted, anyone can validate it quickly. As a result, finding solutions to a puzzle is difficult, because it is resource-intensive, but verifying the solution is efficient because it does not require a significant resource investment.

Controlling the complexity of the cryptographic puzzles ensures that changes to the blockchain happen at a predictable and uniform rate. As the paper discusses below, the immutability of the blockchain comes from the fact that after a block has been added, changing this previously written block requires increasingly more physical resource investment and exponentially decreasing probability of a successful attack as every new block is added to the chain.

2.2 Bitcoin: Cryptocurrency and Digital Payments System

One of the most important requirements of a digital currency (not backed by any physical object) is to prevent *double-spending*, in which the same asset (e.g., bitcoin) is used in two different transactions. This requires that every participant must be aware of all transactions that happen in the system, and that the information about bitcoin transactions are resistant to censorship and manipulation. Achieving these two properties results in all participants sharing the same record about the status of assets (i.e., the amount of bitcoin) controlled by all other participants—they achieve *consensus*. Therefore, the main security property in the bitcoin payment system is not confidentiality, but integrity and authenticity of information. To achieve this, bitcoin depends on two main components: first, immutable data storage (a ledger); and second, data distribution (a communications network).[8]

Bitcoin's blockchain has strict security requirements in terms of data integrity: the stored blocks must be protected against intentional manipulation. To achieve this objective, each block also includes a reference to the previous block, which enables *chaining*—blocks follow a specific, immutable order. A simple analogy is that of a book, in which pages have numbers to help guide the flow of reading and ensure that no page is skipped or added. Instead of page numbers that are independent of the page content, however, the blocks use uniquely defined references generated by applying cryptographic algorithms (such as hash functions) on the block content and the reference of its predecessor block.[9] As a result, if the content of a block changes, the reference of that block also necessarily changes, thereby breaking the blockchain, as the successor block's reference would not match. By using this chaining property, bitcoin users are able to efficiently validate the internal consistency of the blockchain.

Blocks are generated through the mining process discussed above. In bitcoin, the mining process is required for two reasons: it serves to aggregate and add new transactions to the blockchain; and it also generates new bitcoins. Aggregating recent transactions into blocks and adding them to the blockchain is made computationally very expensive; in order to do this, a participant (also called a *miner*) needs to invest the energy required for the necessary computations. This process is incentivized: the first participant who successfully generates a valid block is rewarded by receiving a new bitcoin.

To avoid detection of manipulated data, an attacker would

8 For a good summary, see Anthony Lewis, "A Gentle Introduction to Blockchain Technology," BitsOnBlocks, September 2015, https://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/.

9 This example is taken from Lewis, "A Gentle Introduction to Blockchain Technology."

need to reconstruct the entire set of blocks that was added to the blockchain after the manipulated one, because they all depend on it and their references would need to be recalculated to fit the references of the manipulated data. In the bitcoin blockchain (and most other public blockchains), the level of complexity of such an attack is comparable to the complexity of either attacking the main cryptographic algorithms or recomputing multiple block signatures. Given that they rely on PoW or other means of ensuring that creating even a single valid block requires significant resources, successful attacks of this sort are practically impossible under certain assumptions that this paper discusses in the next section.[10]

The ability to share information about past bitcoin transactions is another important property for guaranteeing the integrity of the bitcoin system. Without it, a double-spending attack would be simple: after spending bitcoins, the attacker could block the propagation of that information; the transaction would not be stored in the blockchain and legitimate users might not be aware that this bitcoin has already been spent. Therefore, the main challenge of the data distribution protocol is to enable *robust* communication between the bitcoin participants.[11] In contrast to conventional client-service communication networks, which assume that the data is stored on a server, bitcoin uses a peer-to-peer network. In such a network, no central server exists; instead, data are replicated many times over. In the case of bitcoin, each "peer" in the network stores all the data. This does not create storage problems because blocks store hashes, which are only about 160 bits long. Yet, a potential security problem occurs if two or more peers create a block (consisting of different lists of transactions) at the same time, which raises the question of which block should be considered valid and written in the blockchain. This situation can arise from both well-behaved peers (e.g., due to network delays which affect the propagation of transactions) or misbehaved peers (e.g., attempting to hide legitimate transactions or to introduce fake transactions). To resolve such situations, the bitcoin's blockchain makes decisions based on consensus, according to the *longest-chain rule*. This rule stipulates that the peers should accept the block that contains the longest chain, i.e., it has most of additional blocks chained to it.[12]

2.3 Theoretical Attacks on Bitcoin

Bitcoin's mining process creates a theoretical vulnerability in the form of a so-called *51-percent attack*, which is based on the assumption that a single entity contributes the majority of the computational power required for block mining. For example, assume that miners are able to control more than 50 percent of the overall computing power in a blockchain. In this case, they would be able to manipulate new blocks, or transactions that are not yet written in the blockchain. The attackers would therefore be able to select which transactions would be written to the blockchain and which would not, enabling them to reverse certain transactions. As a result, bitcoin participants would not be able to check whether a bitcoin has been spent, which could lead to double-spending of bitcoins and a collapse of the currency.

One of the most interesting questions for the security analysis (and as a comparison with other blockchain schemes) is whether a 51-percent attack could change the data already written in the blockchain. That is, would the attacker be able to change the blockchain's history? In case of the bitcoin's blockchain, this is less likely, because the attacker would need to redo all the work that the participants had already invested to build the blockchain up to the block that the attacker would like to change. The further back in history the transactions are, the more difficult it would be to alter them, since other miners would continue extending the existing block. Each such legitimate extension makes it exponentially less likely that attackers could succeed in catching up.

An additional countermeasure against this type of attack is the implementation within bitcoin of "checkpoints" beyond which transactions are hard-coded in the system's software. It is impossible to change transactions prior to these checkpoints. The checkpoint concept is helpful for long-term integrity preservation; both public and private blockchains might benefit from its use.

2.4 Practical Attacks on Bitcoin

There have been some advances in the research on more practical types of attacks against bitcoin's blockchain. While the latter two types of attacks described below might not be applicable to private blockchains, these attacks are directly related to the threat model underpinning the bitcoin design. We thus list some of them to illustrate other factors affecting the security of blockchains:

- **Eclipse Attacks on Bitcoin's Peer-to-Peer Network**

  Ethan Heilman and Alison Kendler introduce an attack scenario that allows an adversary controlling a sufficient number of IP addresses to monopolize all connections

10 See ibid.
11 See ibid.
12 The longest-chain rule is more important than just a means of conflict resolution. This rule makes bitcoin's blockchain independent of authority and based on "work," i.e., resources invested, which results in a different threat model.

used by a legitimate peer.[13] The attacker can then exploit the victim for attacks on bitcoin's mining and consensus system. This is a non-cryptographic attack which is based on abusing network behaviour. Such attacks can occur with both public and private blockchains.

- **Theoretical Bitcoin Attacks Requiring Less Than 51% of the Total Computational Power**

  A paper by Lear Bahack analyzed two kinds of attacks based on two theoretical flaws: the Block Discarding Attack and the Difficulty Raising Attack.[14] By analyzing these two attacks, the study argues that the current theoretical limit of the maximal fraction of total computational power of the attacker is not 50 percent, but less than 25 percent. The paper outlines proposals for protocol change that can raise this limit to be as close to 50 percent as possible. This attack is mostly concerned with PoW based consensus and public blockchains.

- **Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem**

  A paper by Marie Vasek, Micah Thornton, and Tyler Moore offers an empirical investigation into the prevalence and impact of "distributed denial-of-service" (DDoS) attacks on operators in the bitcoin economy, in which many distributed nodes (clients) perform actions with the goal of depleting the server's computational resources.[15] The authors find that 7 percent of all known bitcoin operators have experienced such attacks. Their findings show that currency exchanges, mining pools (groups of miners who share the mining risk and profits), gambling operators, eWallets, and financial services are much more likely to suffer attacks than other online services. For this reason, currency exchanges and mining pools are more likely to have their networks protected against DDoS by using robust content delivery services provided by companies such as CloudFlare, In-capsula, or Amazon Cloud. The authors also find that big mining pools (those with historical mining power of at least 5 percent) are much more likely to be DDoS-ed than smaller pools. The paper discusses attacks on Mt. Gox (a Japanese bitcoin exchange) as a case study for DDoS attacks on currency exchanges. They find that a disproportionate amount of DDoS reports were made during the large spike in trading volume and exchange rates that occurred in the spring of 2013.

13 See Ethan Heilman and Alison Kendler, "Eclipse Attacks on Bitcoin's Peer-to-Peer Network," 24th *Usenix Security Symposium*, (August 2015).

14 Lear Bahack, "Theoretical Bitcoin Attacks with less than Half of the Computational Power," arXiv:1312.7013, IACR Cryptology ePrint Archive, December 2013.

15 See Marie Vasek, Micah Thornton, and Tyler Moore, "Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem," International Conference on Financial Cryptography and Data Security FC 2014: Financial Cryptography and Data Security, Barbados, March 2014, pp. 57–71.

2.5 Blockchain as a Distributed Ledger System

The original idea of bitcoin's blockchain was to serve as a fully decentralized, unpermissioned ledger with the main objective of keeping the information about bitcoin's transactions *public* and *immutable*. While this is the main protection against the problem of double-spending of crypto currencies, the same properties that the underlying blockchain allows can be applied to various other applications. The main advantage of such a blockchain is independence of any pre-defined trust relationships. Given that public blockchains allow achievement of consensus among untrusting participants without any trusted authorities, this removes the risk of a trusted authority acting maliciously (e.g., a bank clerk moving funds without authorization) and results in the increased resilience and robustness of the blockchain. The two main disadvantages of public decentralized blockchains, however, are an increased complexity of the protocols that are needed to incentivize cooperative behaviour; and the complexity of changing any detail of the underlying protocols after they are accepted by participants. For instance, the proposal to increase the number of transactions that are included in a single bitcoin block has been a highly divisive issue in the bitcoin community for some time. While increasing its size would reduce both the transaction costs and the required time to process payments, this proposal has been opposed by a small number of participants with significant computing investments in the blockchain, effectively halting any potential changes in this area.

In the remainder of this section, we analyze other variants of the blockchain technology that have been proposed in attempts to reduce some of the disadvantages of public decentralized blockchains, usually by relaxing some of the core assumptions and design choices that public blockchains rely on.

2.6 Private, Permissioned Blockchains

In contrast to public, decentralized blockchains, many private, permissioned blockchains are being considered within governmental and industrial sectors. Such blockchains have a different trust model: they are based on the authority of trusted peers. Instead of using incentives to stimulate the contributions to the blockchain, the private blockchains use these peers to control access to the blockchain. Any request to write might need permission from a trusted party. As such, the complexity of running private blockchains is much lower compared to public ones, while any potential change to the underlying protocol is significantly easier to achieve as it only requires that the majority of trusted peers to agree. Yet many such concepts are tailored for specific application scenarios and business models; consequently, their security implications and benefits might be more difficult to analyze in generic terms.

In general, a "purist" view on permissioned blockchains is that they are distributed databases enhanced by standard cryptographic primitives. Next, we explore private, permissioned blockchains and their advantages and disadvantages. It is important to mention that there is no unified view on private blockchains; this topic is a source of various debates within academic communities.[16]

2.7 Advantages of Private Blockchains

As mentioned above, if only certain participants can join the peer-to-peer network, the blockchain is considered *permissioned* or *private*. The two main permissioned types of blockchains can be categorized as *consortium-based* and *fully private.* Consortium-based blockchains have trusted owners (government departments, banks, etc.), which make the consensus process simpler. Consider, for example, a consortium of twenty financial institutions with a simple consensus rule that fifteen institutions must sign every block in order for the block to be valid and written to the blockchain. The right to read from the blockchain can be made public, allowing everyone to read it, or it can be restricted to a select group of participants. The ability to read from the blockchain can also be restricted by different levels of abstraction. For example, only the root hashes can be made public, ensuring that individuals without access to the original data cannot learn any new information (as we shall see in Section 3, this is the way that the Guardtime's KSI blockchain is designed). These blockchains are often seen as partially decentralized: members of the public may be able to make a limited number of queries and receive a cryptographic proof of the current state of the blockchain. In contrast, when a blockchain is fully private, the permission to write to the blockchain is centralized and managed by a single organization; permission to read may still be public.

Some of the main advantages of private blockchains are as follows:[17]

- The consortium or company running a private blockchain can easily change the rules of a blockchain, reverse transactions, modify data kept in the blockchain, etc.
- In a consortium, the trusted peers that govern the blockchain are known. This means that the risk of a 51-percent attack arising from large-scale collusion is mitigated.
- Private blockchains are more efficient: only trusted peers, with high processing power, are used to verify transactions.
- Network infrastructure can be planned and controlled. Various network-related problems (such as network delays and connection losses) might be faster to fix.
- If permissions are restricted, private blockchains can provide a greater level of privacy.

The main disadvantage, however, is the reduction of *immutability* guarantees, i.e., the property which makes the data written in the blockchain unchangeable. This property is considered one of the main advantages of the public permissionless blockchains. Indeed, the likelihood of misbehaviour by or successful attacks on trusted peers will have a strong impact on the guarantees provided by the private blockchain. For example, if a malicious actor succeeds in controlling all or the majority of a private blockchain's trusted peers, it might not be able to offer any security guarantees. This paper describes some possible types of attacks on private blockchains in the following section.

2.8 On Attacking Blockchains

A public blockchain, such as bitcoin, is completely decentralized. The system operates based on users' consensus; there is no central point of failure. To attack the system by, for example, manipulating data in the blockchain, the attacker would need to recreate and properly chain all the blocks after the first block whose data are modified—otherwise the attack would be detected though the inconsistency of the blockchain, which any participant can immediately detect. Since adding blocks to a blockchain is a consensus-based process that operates on the PoW concept, the attacker is faced with a tough problem, usually requiring predictably significant physical resources (e.g., time) to overcome. Indeed, if the blockchain is long, the amount of time required for a successful attack renders the task practically infeasible.

The only alternative to avoid such time-consuming computations is to break the cryptographic primitives behind the PoW-based blockchains. Since the blockchain is using the same cryptographic primitives as many other Internet protocols, such as digital signatures and hash functions, breaking these primitives is considered practically infeasible and supported by a strong research community. The threat model in the case of public blockchains is similar to the general cryptographic threat model mentioned above. A successful attack against any of the cryptographic primitives would have an "avalanche effect" because the same primitives are used in Internet security protocols, such

16 There is no generally accepted definition of permissioned blockchains, and there is a heated discussion in the blockchain community about whether permissioned blockchains can be considered blockchains at all. In this section, the discussion is based on Vitalik Buterin, "On Public and Private Blockchains," August 7, 2015, https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

17 See ibid.

as TLS/SSL (Transport Layer Security / Secure Sockets Layer). In conclusion, if the attacker would be capable of breaking the core cryptographic primitives, neither public nor private blockchains can be protected.

Unlike attacks on public blockchains, attacks on private blockchains do not depend mainly on breaking cryptographic primitives. If the trusted peers who grant permissions for writing to the private blockchain are successfully attacked, then the attacker can easily manipulate the blockchain. Thus, in the case of a successful attack against trusted peers, the attacker could strike fast and go unnoticed. While the security model for public blockchains is based on PoW, which assumes that the majority of participants are well-behaved, the security model of private blockchains is less clear: it depends on a particular trust model and the protection mechanisms of the trusted peers. As a result of such tailored and scenario-specific system designs, it is difficult to provide a general statement on the security guarantees offered by private blockchains; such evaluation requires that the specifics of each individual implementation are taken into account. We now provide more detail on one such example.

3 BLOCKCHAIN AND GOVERNMENT SERVICES: THE CASE OF ESTONIA

In the governmental sector, blockchain technology can be used to verify transactions and changes to key registers, transaction logs, agreements, and any other data, which are ordinarily labeled *data-at-rest*. This term comprises all data that are stored in a digital form (databases, spreadsheets, archives, backups, etc.), but excludes any data that are being processed, to which another label applies: *data-in-use*.

Traditionally, the main objective in protecting digital data has been confidentiality—the restriction of access to protected information to only a specific set of individuals. Yet this focus might not be appropriate for data protection in the context of democratic governments; a government's legitimacy may require authorities to increase the transparency and accountability of their processes rather than prioritizing confidentiality. In addition, prioritizing confidentiality requires increasing the complexity of the overall system: confidentiality requires strong secret keys, which in turn require key management protocols that increase overall vulnerability surface and result in various performance challenges. It is important to understand the particular security objectives of the public sector and how to attain them within a democratic context. Estonia's experience with the use of blockchain technology in government offers valuable insights on this question; it also provides a useful benchmark for comparison with other nations.

3.1 Estonia: A Pioneering Case of Blockchain Use

Estonia is one of the world's leading information societies. For more than two decades, the country has been advancing the digitalization of its society. Already in 2000, for example, the country declared Internet access to be a human right, a move that gave impetus to the deployment of Internet access in rural areas, and has driven innovative uses of digital technologies. So far has the country's digital savviness advanced that it has earned the moniker of "e-Estonia."[18]

Estonia aims to propagate digital services and implement technical and legal means to support digital interactions among citizens and the state. Cryptographic technologies are a cornerstone of the security of such interactions. In 2000, for example, the Estonian parliament passed the Digital Signature Act, which made a digital signature equivalent to a hand-written signature; since then, all Estonian authorities have been legally obliged to accept digitally signed documents.[19] Another important part of the legal framework is that it mandates non-duplication for database records (so called *once-only* writing): no information is stored twice; and any update must be performed on the master record. This framework allows for fine-grade logging and auditing of data access and queries of individuals' records. For this reason, there is a clear motivation for utilizing blockchain technology, which guarantees detection of data manipulation attacks, either by internal or external individuals, or even potential state-level actors with access to vast computational and logistical resources.

In Estonian applications of blockchain technology, *Keyless Signature Infrastructure (KSI)* occupies a central place. KSI generates and maintains the blockchain containing the distributed ledger.[20] This technology has been integrated into key government registries, including the business registry, property registry, succession registry, digital court files, and official announcements.

The KSI blockchain is used for both internal and external processes in order to maintain the integrity of records and enable the efficient detection of both intentional and unintentional modifications of data-at-rest. In addition, use of the KSI blockchain enables independent verification by any third party and serves as a long-term forensic "proof of existence." The next section examines the Estonian KSI blockchain from a technical perspective.

18 More specifically, the Estonian information society is based on the following core principles: decentralization, interconnectivity, open platform, and open-ended process. For more information, visit www.e-estonia.com.

19 See Andrew Martin and Ivan Martinovic, "Security and Privacy Impacts of a Unique Personal Identifier," Working Paper No. 4, Cyber Studies Programme, University of Oxford, April 2016, https://www.politics.ox.ac.uk/materials/publications/14987/workingpaperno4martinmartinovic.pdf.

20 For more information, see Guardtime, "KSI Blockchain Technology," https://guardtime.com/technology/ksi-technology.

3.2 The KSI Blockchain and the X-Road

In Estonia, the KSI blockchain is used to provide a *signature service*: a customer transmits the asset's hash value and in return receives a token, which proves its participation in the blockchain. This creates "proof of existence" for any arbitrary piece of digital information. It is important to note that since only the hash value is sent to the KSI service, the original data never leav s customer premises. The main security claims provided by the KSI signatures are proof of integrity, time, and signing entity. The signatures can be independently verified and the system supports a high level of parallelization and scalability.

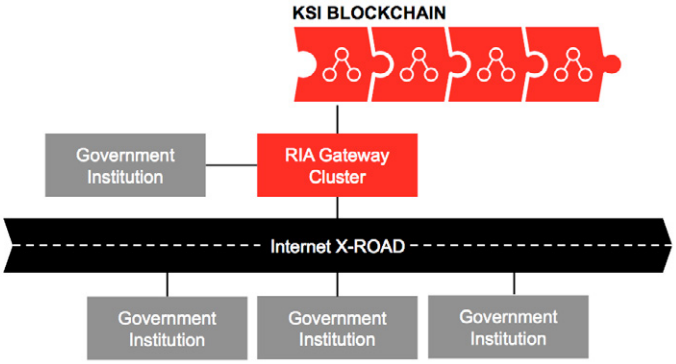
The X-Road is Estonia's interoperability platform; it integrates different interfaces, security services, and the surrounding regulatory framework and serves as the technical backbone of e-Estonia, underpinning various e-services in both the public and private sectors. Its main purposes are to connect different governmental institutions and to facilitate state governance via the use of digital technologies. It is used as the main communication system for government services and supports writing to multiple databases, transmitting large data sets, and performing searches across several databases.[21] The main security guarantees offered by the X-Road are authenticity, integrity, and non-repudiation of exchanged data; high availability of services; and confidentiality of exchanged data.[22] These features enable a communication channel over which data are *digitally signed and encrypted* and by which all incoming data are *authenticated and logged*.

As a citizen portal to government e-services, the X-Road supports the following kinds of vital activity (*inter alia*):[23]

- *Registration services*. The X-Road enables digital transactions in the following areas: residency; electronic declaration of taxes; validation of driving licenses and registered vehicles; application for child benefits and municipal day care; and exchange of documents among government agencies.
- *E-health system*. The X-Road interconnects hospitals, clinics, and other organizations. It implements a unified Electronic Health Record that supplies medical practitioners with information about patients' health while protecting their privacy. For example, the "e-prescription" system allows doctors to create prescriptions and make them immediately available to pharmacies. Patients can then collect their medicines directly from the pharmacy without having to visit the doctor for a hard copy of the prescription.
- *Judicial and police functions*. The "E-File" system uses the X-Road to connect the business processes of courts, police, public prosecutors, prisons, lawyers, and ordinary citizens. Similarly, the Ministry of Interior uses the "e-police" system to provide police officers with access to state registers such as the vehicle register. The police can use this system to check whether a vehicle has been reported as stolen, for example. Consequently, Estonian citizens do not need to carry a driver's license or vehicle documents, because authorities can verify such information online directly from the source.

Figure 1 illustrates the integration of the KSI blockchain into Estonia's X-Road.

Figure 1: Integration of the KSI Blockchain within Governmental Institutions over the X-Road.



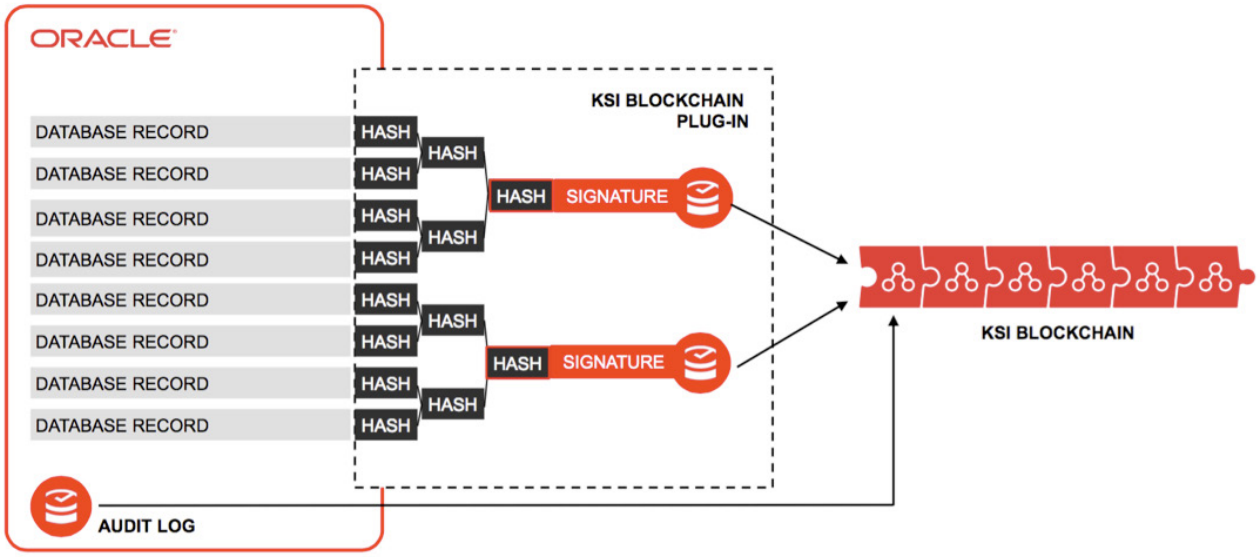
Source: Ivo Lõhmus, Guardtime

3.3 Examples of State Agencies Protecting the Integrity of Data-at-Rest

As explained in the preceding section, the X-Road enables a variety of e-services under a strong security model: all information is digitally signed and encrypted; all incoming data are authenticated and logged. The data protected by the X-Road, however, are *data-in-transit*—that is, the information is required for certain processes, after which it must be securely stored (written back into the database), which renders it *data-at-rest*. The X-Road itself is insufficient to protect such data-at-rest, because various attack vectors that are independent of it can be used to modify the data that are written into the database. Consequently, the protection of audit information (such as transaction and audit logs) and the maintenance of a history of actions and changes to the databases are crucial. In the midst of an attack, a trustworthy transaction log will help authorities both to detect the attack itself and also to recover the system's original database once the attack has been detected. KSI blockchain technology,

21 See Enterprise Estonia, "X-Road," *e-Estonia.com: The Digital Society*, accessed August 2017, https://e-estonia.com/component/x-road/.
22 See Cybernetica, "X-Road," accessed August 2017, https://cyber.ee/en/e-government/x-road/.
23 See Enterprise Estonia, "X-Road."

Figure 2: Protection of Database Records and Audit Logs with the KSI Blockchain Technology.
Source: Ivo Lõhmus, Guardtime.

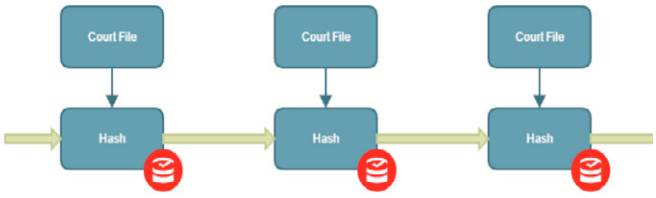


therefore, plays a valuable role in providing strong *integrity guarantees* and enabling efficient detection of changes in stored data.

Figure 2 depicts an example of integration and protection of data-at-rest via the KSI blockchain in the context of the Oracle database system, one of the core database technologies worldwide. In this system, an audit log (or transaction log) containing entries such as a time stamp, user login information, and references to accessed and modified resources, is written to the KSI blockchain, together with the hashes of the database records. This method results in two important integrity benefits: first, each modification in the database record can be detected and the integrity of data verified; and second, changes in the data can be verified from the transaction and audit logs, which are themselves protected by the blockchain.

Figure 3 illustrates the use of blockchain in Estonia's Digital Court System. Estonian courts can protect various types of data by writing their hashes to the KSI blockchain, which guarantees their integrity. The system enables transparent auditability, makes records impossible to delete without detection, and supports legally sound forensic evidence.

Figure 3: The Estonian Digital Court System.



Source: Ivo Lõhmus, Guardtime.

The Estonian e-Health Authority has implemented other innovative uses of blockchains. It has partnered with the systems engineering firm Guardtime to protect the integrity of more than one million health records.[24] In this context, the application of blockchain technology will enable independent and legally sound proof-of-record existence and database integrity for internal, external, and regulatory compliance purposes.

Yet another example of the technology's use involves the Estonia Succession Registry, in which electronic records and associated metadata are chained to the previous record and signed (i.e., written to the KSI blockchain). The chaining of the records offers provable ordering: it makes it impossible to delete a record without being detected (see Figure 2).

24 Ian Allison, "Guardtime Secures over One Million Estonian Healthcare Records on the Blockchain," *International Business Times*, March 4, 2016, http://www.ibtimes.co.uk/guardtime-secures-over-million-estonian-healthcare-records-blockchain-1547367.

The list of Estonian State Agencies that are currently implementing and utilizing KSI blockchain technology within their respective service domains is as follows:

- Healthcare Registry
- Property Registry
- Business Registry
- Succession Registry
- Digital Court System
- Surveillance / Tracking Information System
- State Gazette (official laws and regulations system)
- Official State Announcements

3.4 A Technical Overview of the Keyless Signature Infrastructure (KSI)

What technical features underpin the KSI blockchain? As a prerequisite to support securing the vast number of signing operations happening at any given moment, it is necessary to aggregate the operations before updating the blockchain while ensuring that all the required integrity checks are still possible. The technology relies on Hash Trees (HT), a data structure that can be used to protect the integrity of documents using cryptographic hash functions, as shown in Figure 4.

The KSI uses digital time-stamping to create and store proofs of existence: a user sends a cryptographic hash value of a document to the service, which in turn stores it in the HT. The user then receives a signature token as a receipt to provide proof that the data have been stored in the HT. The signature token is also used as a starting point (a *leaf*) to reconstruct the path through the HT. Figure 4 below illustrates this procedure.

In the case of the KSI, an HT is created in each round, which is defined by a time interval. All requests received during the same time interval are stored within the same HT. The top hashes from each round are linked together in a global HT called a *hash calendar*. The top hash of the calendar is periodically published and distributed on a hard-to-modify medium, such as a widely-read physical newspaper. This ensures that even the complete compromise of the KSI infrastructure by the adversary cannot "modify history," because the physically published top hashes are immutable owing to their wide distribution and physical nature.

The main operational challenges of such an infrastructure are *performance* and *scalability*. The KSI introduces three main components to cope with these challenges: aggregation networks, core clusters, and KSI gateways, which the paper describes in detail below.[25]

3.4.1 Aggregation Networks

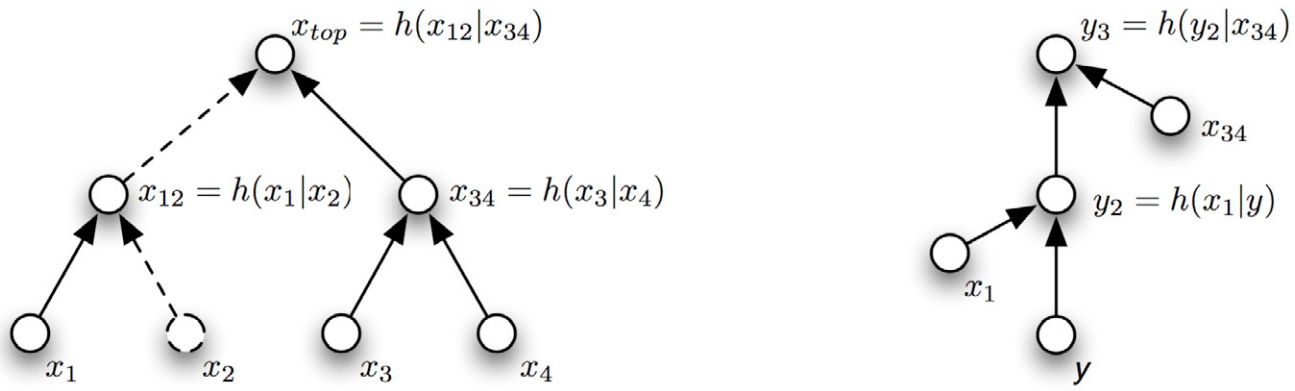
Aggregation networks are the part of the KSI subsystem that is used to create HTs from incoming requests. The top hash of each tree is sent upstream, either for further aggregation (within the aggregation network) or into the core cluster. The aggregators work in rounds of equal duration; the requests received during the round are aggregated into the same HT. After receiving a response from an upstream component,

25 For more details, see Ahto Buldas, Andres Kroonmaa, and Risto Laanoja, "Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees," Proceedings of the Eighteenth Nordic Conference (NordSec 2013), Pp 313 - 320.

Figure 4: A Hash Tree as Used in the Keyless Signature Infrastructure.

Note: Hashes of several documents (x_1–x_4) are stored as leafs in the HT. The intermediate nodes are generated by hashes, which are computed over aggregated hashes from the layer below. The top hash (x_{top}) represents the overall HT. On the right is the verification of the document y. If $y_3 = x_{top}$, then it can be assumed that y was in the original HT and has not been modified.

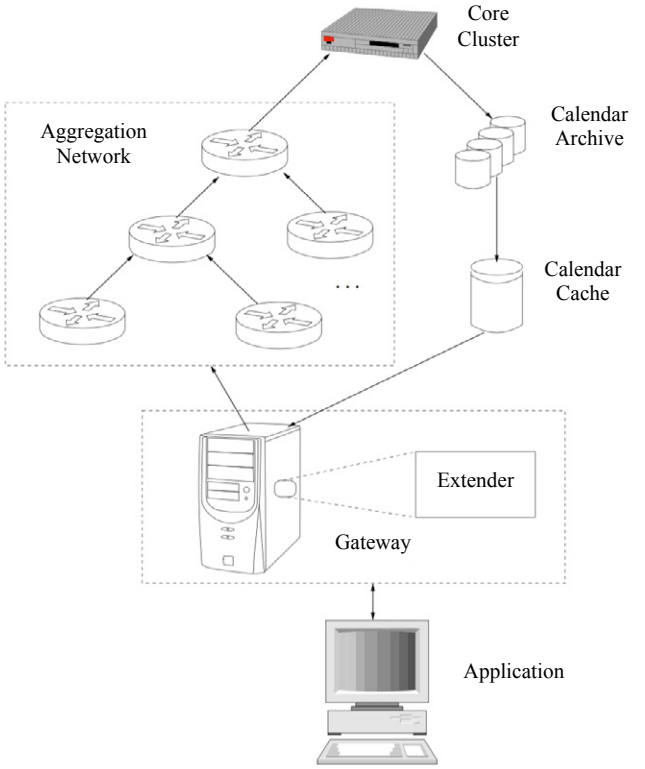
Source: Ahto Buldas, Andres Kroonmaa, and Risto Laanoja, "Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees".



an aggregator delivers the response to all aggregators at the lower levels together with the hash paths of its own tree, which are then used to verify the signature token.

The availability of the aggregators is a system-critical factor; a successful attack on them would prevent users from reading and writing to the blockchain. To increase the availability of the aggregators' service and to avoid single points of failure, the KSI relies on redundancy: the aggregation network is made of geographically dispersed clusters of aggregation servers. Figure 5 illustrates the structure of the aggregation networks.

Figure 5: The main architecture of the KSI's aggregation networks.



Note: The application performs the first hashing step, which also generates the signing request. The signing request is sent to the gateway, which forwards it to the aggregation network. The aggregators build the hash tree and pass the top hash values upstream. Once the top hash reaches the core cluster, it is stored in the calendar database. The core cluster is also responsible for reaching consensus among the servers. The values from the calendar database are also available from the calendar cache. The cache is then used by extenders during the verification service.

Source: Nitesh Emmadi and Harika Narumanchi, "Reinforcing Immutability of Permissioned Blockchains with Keyless Signatures' Infrastructure," Proceedings of the 18th International Conference on Distributed Computing and Networking, 2017.

3.4.2 Core Clusters

Core clusters are distributed synchronized systems responsible for achieving consensus on the top value hashes from aggregation periods. A core cluster permanently stores the top hashes in the calendar database and returns them to the aggregation network (as part of the *signature token*). The core cluster is also responsible for time synchronization, which represents the issuing time of each signature token.

The aggregation servers propagate their top hash values to all core nodes. A multi-party consensus protocol is used to detect discrepancies in the submitted top hashes; because even among honest participants, different errors or timing collisions can occur, only the values that are identical from the majority of voting core servers can be written in the calendar database.

3.4.3 KSI Gateways

The KSI gateways are protocol adapters: they serve as interfaces for different applications that use the KSI blockchain. The gateways implement the first level of aggregation, because the workload can be predicted and does not require high bandwidth channels. The gateways also implement an extender service that provides a *signature verification* (using a signature token as an input). The extender service has access to a fresh copy of the calendar database and provides missing hash values that are necessary to build full hash chains from signed data to the latest published hash value. The client validates the hash chains created with the help of the extender. The token validity is decided at the application layer; the gateway must not be treated as a trusted party.

3.5 The KSI Blockchain's Security Objectives

The main security objective provided by Estonia's use of the KSI blockchain is data *integrity*. As discussed above, this involves guaranteeing that no information can be modified undetectably. The KSI blockchain provides an efficient way of detecting manipulation of data-at-rest; the likelihood of detection is directly related to the frequency of integrity validation requests.

Because only the hashes are stored in the KSI blockchain, there is a preservation of data *privacy*; the original document cannot be recreated from these hashes. Such an approach, however, means that other security measures need to be provided in order to ensure *data availability*, which we discuss next.

3.5.1 Data Availability

As discussed above, the KSI blockchain stores cryptographic representations of data using one-way cryptographic hash

functions, meaning that the blockchain offers no mechanisms to assist in data availability, and data cannot be recovered from the blockchain. Yet data availability is an important requirement for crucial governmental records. Furthermore, without available data, it is difficult to resolve the problem of having different versions of the blockchain. Different versions might occur without malicious behaviour; they can exist due to network-related communication problems, such as packet loss or delay, which results in the loss of a transaction order. Hence, as Chief Architect of the Estonian Information System Authority Andres Kütt explains, one of the main questions that arises in this context is the following: "Assuming imperfect communication, how does one maintain and prove exactly one understanding of registry entries and of their order?"

A conventional way to increase resilience to the loss of data availability—whether unintentional due to faults, or intentional due to malicious behaviour—is by way of *disaster recovery*, which is based on increasing the redundancy of data and equipment. This can be achieved by various trade-offs between recovery time and running costs as a result of physically cloning only the data storage facilities (*cold sites*), or also cloning equipment that is necessary to immediately continue serving the data (*warm sites*) in case of failure.

In general, a significant physical distance between the recovery sites is required to minimize the effect of catastrophic events. This requirement poses a problem for geographically small countries such as Estonia. For this reason, Estonian authorities have developed the concept of *data embassies*, which involve the maintenance of hosting facilities outside of the national territory (yet within the government's legal jurisdiction).[26] Such data embassies allow for copies of key registries to be stored and used in case of a major availability incident or any other event that generates different versions of the blockchain. At present, the implementation of data embassies has just begun; several legal and technical challenges remain unsolved. The concept, however, offers an intriguing and promising approach to disaster recovery in support of blockchain technology.

3.5.2 Quantum-Attack Resilience and the KSI Blockchain

Current research suggests that the main challenge of making systems resilient against quantum-computation attacks is to avoid the use of a *trapdoor function,* or a function that is easy to compute in any one direction yet difficult to compute in the opposite direction without special information. Trapdoor functions are the main building blocks of conventional asymmetric cryptography systems that underlie the majority of secure communications in today's world. A recent study by Ahto Buldas, Risto Laanoja, and Ahto Truu describes the quantum-resilient properties of the KSI.[27] The authors discuss the case of quantum-computational attacks and their impact on the security of the KSI blockchain. They claim that the KSI's resilience to such attacks involves avoiding trapdoor functions, using only cryptographic hash functions, and publishing the hashes as the KSI's main security mechanisms.

4 BLOCKCHAIN AND GOVERNMENT SERVICES: OTHER COUNTRIES

Several other countries have begun experimenting with blockchain implementation in their own governmental services, though none of them has integrated the technology to the extent that Estonia has done. Below the paper briefly discusses other national contexts.

4.1 Britain

A recent report by the British Government's Chief Scientific Advisor provides interesting case studies of integrating blockchain technology into governmental processes in Britain.[28] These cases include, for example, novel payment models for HM Treasury and the Department for Work and Pensions (DWP). The general idea behind the use of blockchains involves the registration and payment processes of governmental grants and benefits. As an example of potential improvements, it is estimated that out of around £166 billion of taxpayers' money that DWP pays in welfare support per year, about £3.5 billion is overpaid through fraud, claim errors, and official errors—an astonishing loss of public money. In this case, the blockchain technology provides an alternative and potentially superior disbursement method: it enables end-users to receive benefits directly into their digital wallets, reduces the transaction costs to banks and local authorities, and could help to increase the transparency of public expenditures. Such a solution could also be integrated with other systems in order to reduce fraud and errors in the delivery of public benefits.

26 Microsoft and Estonian Ministry of Economic Affairs and Communications, "Implementation of the Virtual Data Embassy Solution", 2015. https://www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf.

27 For more information, see Ahto Buldas, Risto Laanoja, and Ahto Truu, "Keyless Signature Infrastructure and PKI: Hash-Tree Signatures in Pre- and Post-Quantum World," *International Journal of Services Technology and Management*, Vol./No. 23 (January 2017).

28 See UK Chief Scientific Advisor, "Distributed Ledger Technology: Beyond Block Chain," January 19, 2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

Recently, Guardtime and Future Cities Catapult announced a partnership to develop blockchain-based cybersecurity services for critical British infrastructure. Future Cities Catapult, the British-based centre of excellence for "smart city" innovation, will initially focus on building prototype applications to enhance the resiliency, security, and reliability of critical infrastructure. These projects, which rely on Guardtime technology, include flood defence systems, nuclear power, and the electricity distribution grid. Catherine Mulligan, head of Digital Strategy and Economics at Future Cities Catapult, stated: "Guardtime's unique permissioned blockchain approach to large scale system integrity has tremendous potential to enhance the security of British critical infrastructure and we are excited to work with the Guardtime team to build solutions that will play a key part in the government's industrial strategy and showcase to the world how cities can be smarter in the future."[29]

4.2 Sweden

Sweden, too, has begun to explore the use of blockchain technology. The Swedish Mapping, Cadastre, and Land Registration Authority has partnered with private companies such as Telia, ChromaWay, and Kairos Future to use the technology to support real estate transactions. At present, the project is still in an early phase of feasibility testing. According to a report from July 2016, the blockchain-based project seeks to achieve the following objectives:[30]

- *Increased transparency of transactions*. The Swedish government is involved in only a few steps at the end of transactions, while other steps are carried out between private parties and thus are not visible to the public or other stakeholders.
- *Increased efficiency of the overall process*. Currently, the time between the signing of a legally binding contract, receiving the bill of sale, and making an approval takes three to six months. Having a publicly verifiable record will simplify the overall process and decrease the time required to complete the transaction.
- *Decreased complexity of the overall process*. Due to the problems mentioned above, the stakeholders have created their own complex workarounds for agreements between them, with the aim of minimizing the likelihood of errors (the transactions in this context carry a large financial value). Blockchain technology, together with an appropriate IT architecture, might solve many of these issues and mitigate weaknesses in processes and systems.

The project reportedly moved into its second phase, which involves researching how the technology can be integrated with banks for the verification of contracts.[31] Despite the successful progress, however, there still remain legal and technical obstacles that need to be overcome before the system can be fully deployed. One obstacles, for example, is the legal requirement that such contracts require physical signatures on paper.

4.3 Japan

In June 2017, Japan's Ministry of Internal Affairs and Communications released a statement that they plan to test a blockchain-based system for processing government tenders.[32] The system seeks to simplify the process significantly for both the private sector and the government by allowing the agencies that are issuing the tenders to electronically gather necessary information, such as tax payment certificates. This initiative is scheduled to launch in 2018. It is part of the country's broader vision to use blockchain technologies across digital services.

4.4 China

Following the inclusion of blockchain technologies in their "Thirteenth Five-Year Plan" in 2016, the Chinese government has announced that they have plans to start using blockchain technology in tax collection and the issuing of invoices.[33]

4.5 The United States

The General Services Administration, the U.S. government's main logistical agency, is looking for contractors to assess how blockchain technologies can be integrated into its

29 See Martin Ruubel, "Guardtime and Future Cities Catapult Partner to Develop Blockchain-based Cybersecurity for UK Critical Infrastructure," Press Release, Guardtime, December 14, 2016, https://guardtime.com/blog/guardtime-and-future-cities-catapult-partner-to-develop-blockchain-based-cybersecurity-for-uk-critical-infrastructure.

30 See Swedish Mapping, Cadastre and Land Registration Authority, Telia, ChromaWay, and Kairos Future, "The Land Registry in the Blockchain: A Development Project with Lantmäteriet," press release, ChromaWay, Sweden, July 2015.

31 See "Sweden Moves to Next Stage With Blockchain Land Registry" Press Release, CoinDesk, March 30, 2017, https://www.coindesk.com/sweden-moves-next-stage-blockchain-land-registry/.

32 See "Japan looks to blockchains for more secure e-government systems," Press Release, Nikkei Asian Review, June 29, 2017, https://asia.nikkei.com/Politics-Economy/Policy-Politics/Japan-looks-to-blockchains-for-more-secure-e-government-systems.

33 See "China Will Experiment with Using Blockchain to Collect Taxes," Press Release, MIT Technology Review, August 7, 2017, https://www.technologyreview.com/the-download/608570/china-will-experiment-with-using-blockchain-to-collect-taxes/.

contract bidding system.[34] The system envisioned is described as "a permissioned ledger that uses multiple cloud platforms for redundancy and high-availability and key management."

5 CONCLUSION

The use of blockchain technologies in public life and governmental services offers notable efficiency and security benefits. From a technical perspective, it enables simple and efficient methods of recordkeeping that are resilient against strong adversarial models.

Both the public and private sectors are currently considering ways of using and implementing various instantiations of the blockchain technology. On the one hand, the private sector is attracted to the efficiency and low cost, given that the centralized nature of traditional commerce does not scale well. The decentralized approach, however, in which information is shared, has conventionally been considered risky for businesses. The technologies presented in this paper promise to resolve many of these issues. Blockchains are able to preserve the integrity and confidentiality of records stored within it using well-established cryptographic methods; at the same time, their distributed nature enables different stakeholders to "own" it. Consequently, this technology fulfils the basic principle of economic models of sharing economies and free markets.

Yet there are also notable challenges. From a technical perspective, perhaps the biggest challenge is to understand the overall security guarantees provided by such systems. Some blockchains are mostly concerned with integrity verification; other security objectives also need to be provided with high availability requirements and strong threat models. In particular, private blockchains might vary greatly in their capabilities. Their security evaluation will depend on understanding the concrete consensus mechanism and implications of other security components that implement authentication and authorization services. In this context, another important challenge is data availability.

Storing only hash values in private blockchains (as is the typical case for Guardtime's KSI infrastructure) helps to preserve data privacy—yet other mechanisms are required to guarantee the availability of the data itself.

As discussed above, the public blockchains that are based on PoW protocols have inherent "self-healing" properties based on a resource investment that the system rewards. In contrast, private blockchains, such as the one deployed in Estonia's governmental services, avoid these often energy-inefficient mechanisms. Private blockchains are optimized for specific application scenarios and rely on preexisting trust relationships; only trusted nodes are allowed to write to blockchains. This approach enables higher efficiency, but it comes with a price: security guarantees of private blockchains cannot be easily generalized. Their capabilities and resistance to strong adversaries depend on the concrete trust models and implemented security mechanisms that are used to protect the peers from insider and outsider attacks.

Compared to Estonia's use of blockchain technology in support of governmental services, other governments are still at an early, largely conceptual stage of planning. Most benefits of the technology in these countries still relate to potentially increased transparency and more efficient workflows. Thus there is still a notable degree of uncertainty in these countries about the technology's implementation, especially because it cannot be treated as an isolated component of the national IT infrastructure, but rather as a dependent component in a larger system of governmental services.

The Estonian government's ample and varied use of private blockchains to support public services reveals the technology's many potential advantages—ranging from increased transparency to process efficiency to quantum resilience. Yet an overall system security analysis is required to provide conclusive answers to outstanding questions about the technology's viability. These questions include the following: How resilient is the consensus mechanism to various forms of attack? What security guarantees can be provided? Answers to these important questions will require further research—in particular, detailed case-by-case analyses of the technology's performance under realistic threat models, such as the presence of insider threats or the threat of nation-state cyberattacks that undermine the availability of blockchain-related services.

34 See "US Government Seeks Blockchain Solutions for Contract Bidding System," Press Release, CoinDesk, June 22, 2017, https://www.coindesk.com/us-government-blockchain-contract-bidding/.

CENTRE FOR
TECHNOLOGY &
GLOBAL AFFAIRS

UNIVERSITY OF
OXFORD

www.ctga.ox.ac.uk

ABOUT THE CENTRE FOR TECHNOLOGY AND GLOBAL AFFAIRS

Oxford University's Centre for Technology and Global Affairs produces interdisciplinary research on the transforming impact of new technology on international relations, government, and society.

Our academic mission is (a) to shape scholarly debates and opinions in the interdisciplinary study of new technological developments; and (b) to support and train researchers and practitioners in this field, with a special emphasis on integrating technological issues into political science.

Our policy-oriented mission is (a) to provide leadership in creating new knowledge on practical problems affecting the security and welfare of governments, citizens, and private enterprises; and (b) to influence major policy decisions and opinions in these arenas.

The Centre is based in the Department of Politics and International Relations at Oxford University. It is supported by core funding from Kluz Ventures.

Centre for Technology and Global Affairs
Department of Politics and International Relations
University of Oxford
Manor Road
Oxford OX1 3UQ
United Kingdom

UNIVERSITY OF
OXFORD

DPIR
DEPARTMENT OF POLITICS &
INTERNATIONAL RELATIONS