Blockchains: Design Principles, Applications, and Case Studies

Working Paper No.7 (DRAFT)

(Supporting material for the Training Session No. 5:

Cyberspace, Politics, and Society)

Professor Ivan Martinovic

Associate Professor of Computer Science

University of Oxford

ivan.martinovic@cs.ox.ac.uk

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

European Union
European Social Fund

Investing
in your future

Introduction

A blockchain is a type of distributed database comprising blocks of data, each of which contains a list of previous transactions. Blockchain technology is the subject of intense and growing attention among governments, technology developers, and private investors. The UK government, for example, has recognised that the technology "could transform the conduct of public and private sector organizations."[i] In Estonia, private firms are planning to use blockchain-related technology in conjunction with digital ID cards to conduct shareholder voting.[ii] 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."[iii]

Yet, the research and deployment of practical applications remains limited. As one small survey of the literature observed, less than 20 per cent of existing academic publications on the technology focus on its applications.[iv] The most prominent contemporary applications are crypto-currencies such as Bitcoin.[v] This paper, however, will not focus on crypto-currencies; rather, it uses Bitcoin as an example to illustrate the underlying principles and properties that allow blockchains to function: the creation, distribution, and protection of distributed ledgers and 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.[vi] The paper will also discuss the technology's potential application in other contexts and countries, such as the United Kingdom, 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?

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 a higher transparency to process efficiency and increased resilience against various cyber attacks. Overall, the paper aims to provide an overview of the technical rudiments and practical applications of blockchain technology, with a special emphasis on its use to support Estonian government systems and applications.

Finally, it is important to emphasise that many aspects of blockchain-based technologies are still part of an on-going research. One of the main challenges in introducing blockchain-based technologies is finding a balance between various, orthogonal system objectives, such as, security vs. performance. For this reason, many so-called private, permissioned blockchains are currently being designed with the objective to keep the costs of running a blockchain low. In these cases, the security guarantees are difficult to generalise and they depend on a concrete blockchain implementation.

A Brief Introduction to Blockchain Technology

In 2008, the digital cash called Bitcoin—probably the most well known digital currency—was invented. While Bitcoin is a recent invention, the underlying technology that enables it has existed for decades. 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 components of the Bitcoin system are based on well-understood and established cryptographic constructs.

The ensuing discussion introduces the main security objectives and cryptographic constructs which are used to achieve these objectives within realistic threat models. The underlying cryptographic primitives will be used later to discuss blockchain threat models and to conduct a comparative analysis of different approaches in designing blockchains.[vii] In the following section, we briefly introduce some of the technical concepts which are important for the understanding of this report:

Confidentiality is used to keep the content of information accessible only to individuals who are authorised to access it. The authorisation 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 unauthorised 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 cryptographic primitives, the most common of which are cryptographic *hash functions*. The cryptographic hash functions are security primitives which 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 security primitive can be used to provide evidence that the data has not been modified.

Authentication can be subdivided into two major classes: *entity authentication* and *data origin verification.* Entity authentication is used by parties to identify each other when entering into a communication. Entity authentication protocols include a claim of identity and methods to verify the claim. Similarly, 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 authorisation 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 there no single authority that grants permissions for reading or writing to the blockchain is required. Such a blockchain is also called *immutable* and it is highly *censorship resistant*. The main complexity of public blockchains comes from 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 authorised entities are able to access them. Traditionally, availability has not been an objective of cryptographic primitives because it is more 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 aspects 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 ecosystems usually require *Proof-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 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. But if a client sends many such requests, 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, because the client's requests can be manipulated so that it seems to originate in different clients.

The Proof-of-Work concept approaches this problem by requesting some commitment (in terms of a resource investment) from the client side. In the context of blockchains, it requires commitment to contribution to the blockchain. This is achieved by solving so-called cryptographic client puzzles, which involves searching for information over a large search space—a laborious task that takes time to solve. With Bitcoin, for example, the participating peers need to invest resources to execute its protocols; this improves the integrity of Bitcoin's blockchain by validating transactions stored within. For Bitcoin's blockchain, finding a solution to cryptographic puzzles means generating a correct block for the blockchain (i.e., collecting transactions and adding them to the blockchain). In Bitcoin's terminology this is called *mining*. An important property of Proof-Of-Work protocols is that 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. In this way, every peer can efficiently verify whether the mining has resulted in the production of the correct block.

Bitcoin's Ecosystem

One of the most important requirements of the digital currency is to prevent *double-spending*. This means that every participant should know the status of Bitcoin, which also implies that the information about Bitcoin transactions should be resistant to censorship and manipulation and should be available to all participants. Therefore, the main security property in the Bitcoin's Ecosystem is not confidentiality but integrity and authenticity of information. To achieve this, Bitcoin depends on two main components: (1) data storage (ledger) and (2) data distribution (communication network).[viii]

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 certain order.

A simplified analogy is that of a book. Pages in a book have numbers which help to guide the flow of reading, but instead of page numbers, the blockchain's blocks use references generated by applying cryptographic algorithms (such as hash functions) on the block content.[ix] If the content changes, the reference of that block would also change, thereby breaking the blockchain. By using this chaining property, Bitcoin users are able to efficiently validate the internal consistency of the blockchain.

To avoid detection of manipulated data, an attacker would 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 reference of the manipulated data. In the Bitcoin blockchain, the level of complexity of such an attack is comparable to the complexity of attacking the main cryptographic algorithms. In other words, a successful attack of this sort is practically infeasible.[8]

The ability to share information about past Bitcoin transactions is another important property for guaranteeing integrity of the Bitcoin ecosystem. 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.[8] 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 questions 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 a situation, the Bitcoin's blockchain makes decisions based on a consensus. The consensus in this case is based on the *longest chain rule*, which stipulates that the peers should always accept updates that also contain the longest chain, i.e., it has most of additional blocks chained to it.[x] Blocks are generated in a process called *mining* – 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 transaction into blocks and adding them to the blockchain is made computationally very expensive – to do this a participant (also called a *miner*) needs to invest energy required for computations and therefore this process is incentivised: the first participant who successfully generates a valid block is rewarded by receiving a new Bitcoin.

Directly related to the mining process is a so-called *51-percent attack*. The *51-percent attack* is a hypothetical attack based on the assumption that a single entity contributes the majority of the computational power required for block mining. For example, assume a miner (or a group of miners) able to control more than 50-percent of the overall computing power. In this case, they would be able to manipulate new blocks, or transactions that are not yet written in the blockchain. The main effect of a 51-percent attack on the Bitcoin's blockchain is that the attacker would be able to select which transactions would be written to the blockchain and which would not, enabling the attacker 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 since it means that the attacker would need to re-invest the work that the participants have 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.

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

There have been some recent advances in research on more practical attacks against Bitcoin's blockchain. While they might not be applicable to private blockchains, these attacks are directly related to the threat model underpinning the Bitcoin design and we list some of them to illustrate other factors affecting the security of the 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 monopolise all connections used by a legitimate peer.[xi] 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. As we see in Section 4 below, the problem of branching (i.e., having different versions of blockchain) might result not only from malicious behaviour but also from various availability-related problems, such as network delays.

- **Theoretical Bitcoin Attacks with Less than Half of the Computational Power.**

  A paper by Lear Bahack analysed two kinds of attacks based on two theoretical flaws: the Block Discarding Attack and the Difficulty Raising Attack.[xii] The study argues that the current theoretical limit of the attacker's fraction of total computational power essential for the security of the system is not 50 per cent, but less than 25 per cent. The paper outlines proposals for protocol change that can raise this limit to be as close to 50 per cent as possible. This attack is mostly concerned with Proof-of-Work 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.[xiii] The authors find that 7 per cent of all known Bitcoin operators have experienced denial-of-service attacks. Their findings show that currency exchanges, mining pools, gambling operators, eWallets, and financial services are much more likely to suffer attacks than other services. For this reason, currency exchanges and mining pools are more likely to have their networks protected against DoS 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 per cent) 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.

Blockchain as a Distributed Ledger System

As described in the previous section, the original idea of Bitcoin's blockchain was to serve as a fully decentralised, unpermissioned, public ledger with the main objective of keeping the information about Bitcoin's transactions *public* and *immutable*. This is the main protection against the problem of double-spending in the context of crypto-currencies. The main advantage of such a blockchain is independence from pre-defined trust relationships, mitigating the risk if trusted authorities become malicious, which results in an increased resilience and robustness to attacks. The main disadvantage is an increased complexity of the protocols that are needed to incentivise cooperative behaviour. Currently, the Proof-of-Work mechanism results in relatively high transaction fees, which make the overall system energy-inefficient.

In contrast, 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. Yet many such concepts are tailored for specific application scenarios and business models; their security implications and benefits might be more difficult to analyse.

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

Private, Permissioned Blockchains

In contrast to public blockchains, which everyone can read, write transactions to, and participate in the consensus process, there is a wide range of other options on how a blockchain might be designed and implemented. 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 categorised as *consortium-based* and *fully private.* [xiv] Such blockchains would 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, or it can be restricted to a 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 (as we will see in Section 4, this is the way that the Guardtime's KSI blockchain is designed). These blockchains are often seen as partially decentralised: members of the public may be able to make a limited number of queries and receive a cryptographic proof of the blockchain state. The fully private blockchain means that the permission to write is centralised and managed by a single organisation, while the read permission may still be public.

Some of the properties that are considered to be the main advantages of private blockchains are as follows:[xv]

- The consortium or company running a private blockchain can easily, if desired, change the rules of a blockchain, revert transactions, modify data kept in the blockchain, etc.
- 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.
- The private blockchain is more efficient: only trusted peers, with a very 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 lack of *immutability,* 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 the trusted peers, the private blockchain might not be able to offer any security guarantees.

On Attacking Blockchains

A public blockchain, such as Bitcoin, is completely decentralised. The system operates based on users' consensus; there is no central point of failure. To attack the system, for example, by manipulating data in the blockchain, the attacker would need to reconstruct and add all the blocks that have changed as a result of the attack—otherwise the attack would be detected though the inconsistency of the blockchain. Since adding blocks to the blockchains is a consensus-based process that operates on the Proof-of-Work concept, the attacker is faced with a tough problem requiring much time to overcome. Indeed, if the block, which an attacker wants to change, is old, 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 in Section 2. 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 as TLS/SSL. In sum, if the attacker is capable of breaking cryptographic primitives, neither public nor private blockchains can be protected.

Yet in the case of private blockchains, the attacker might have other options. Attacks on private blockchains do not depend only 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.

In summary, the security model for public blockchains is based on Proof-of-Work, 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 design, it is difficult to provide a general statement on the security guarantees offered by private blockchains.

Blockchains and Governments: Estonia and Other Case Studies

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 labelled *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, or the restriction of information to 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. In addition, prioritising 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.

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 digitalisation 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 which 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."[xvi]

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.[xvii] 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 introducing blockchain technology, which would guarantee detection of data manipulation attacks.

In Estonian applications of blockchain technology, *Keyless Signature Infrastructure (KSI)* occupies a central place. KSI generates and maintains the blockchain containing the distributed ledger.[xviii] 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, the use of KSI blockchain enables independent verification by any third party and serves as a long-term forensic "proof of existence."

The next section discusses the Estonian KSI Blockchain from a more technical perspective.

The KSI Blockchain

In Estonia, the KSI Blockchain is used to provide a *signature service*: a customer transmits the asset's hash and in return receives a token, which proves participation in the blockchain.

This creates a so-called proof of existence. Data never leave customer premises, because only the hash is sent to the KSI service. 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 parallelisation and scalability.

X-Road

The X-Road is Estonia's interoperability platform; it integrates different interfaces, security services, and the surrounding regulatory framework. Its main purpose is to connect different governmental institutions and to facilitate state governance via the use of digital technologies. It is used as the main communication system of government services and supports writing to multiple databases, transmitting large data sets, and performing searches across several databases.[xix] 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.[xx] These features enable a communication channel over which data are *digitally signed and encrypted* and by which all incoming data are *authenticated and logged*. The X-Road system is the technical backbone of e-Estonia: it underpins various e-services in both the public and private sectors. As a citizen portal to government e-services, the X-Road supports the following kinds of vital activity (*inter alia*):[xxi]

- *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 organisations. 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. (Remarkably, 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.)

Protection of the Integrity of Data-at-Rest

As described 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 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 attacks 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 state. KSI blockchain technology, therefore, plays a valuable role in providing strong *integrity guarantees* and enabling efficient detection of changes in stored data. Figure 1 depicts the general integration of the KSI blockchain structure into governmental services, in particular, the crucial “X-Road” system.

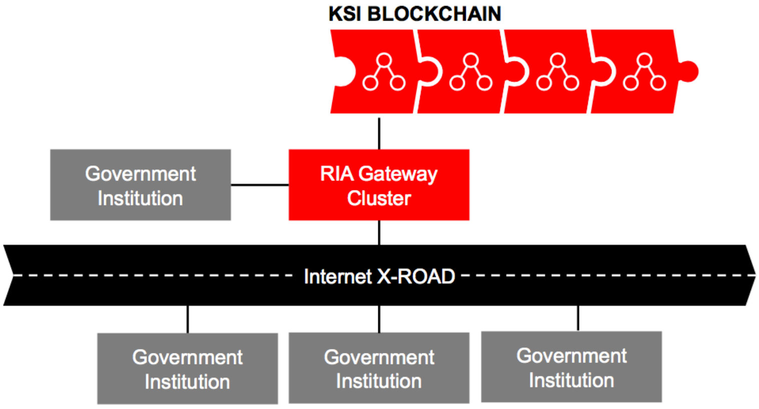


Figure 1: Integration of the KSI Blockchain within governmental institutions over X-Road. Source: Ivo Lõhmus, Guardtime.

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

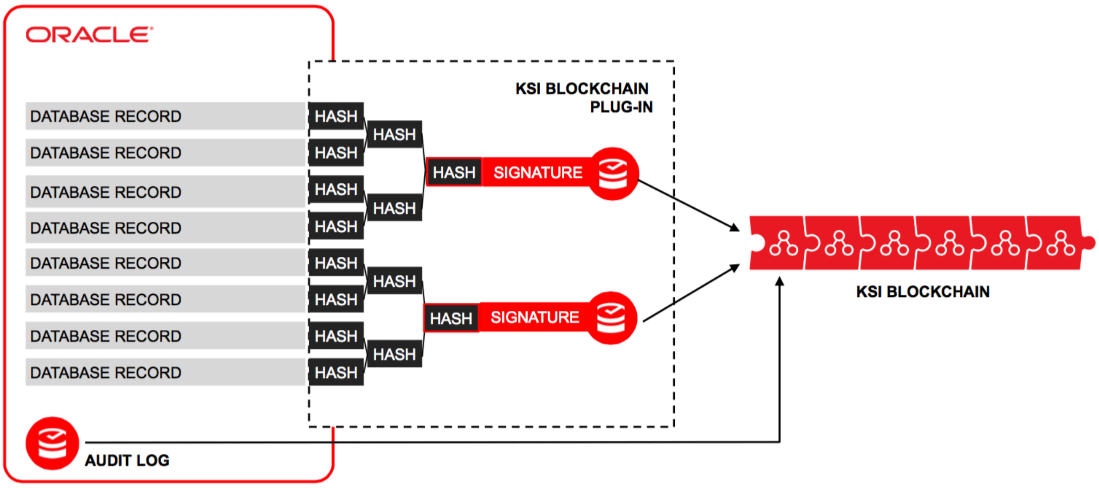


Figure 2: Protection of database records and audit logs with blockchain technology.

Source: Ivo Lõhmus, Guardtime.

Figure 3 below provides another example: 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. Similarly, as portrayed in Figure 6, all files associated with the Estonian Business Registry are hashed and written to a secure blockchain.

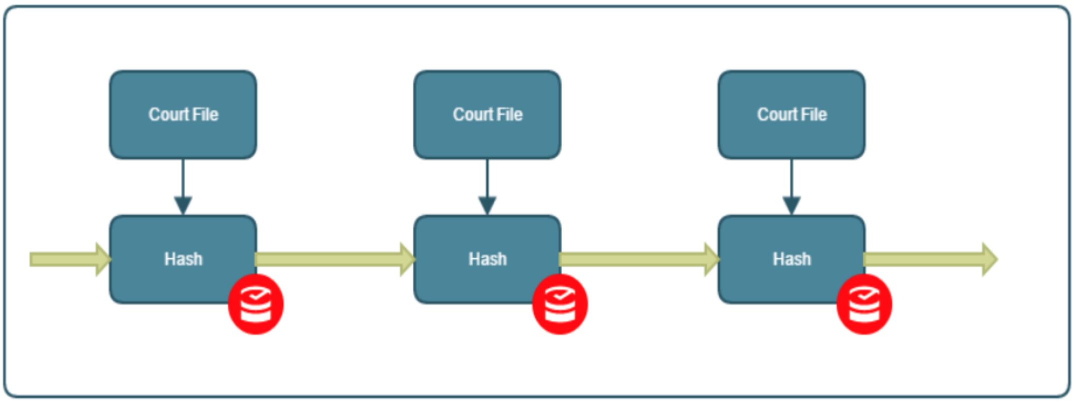


Figure 3: Estonian Digital Court System. Source: Ivo Lõhmus, Guardtime.

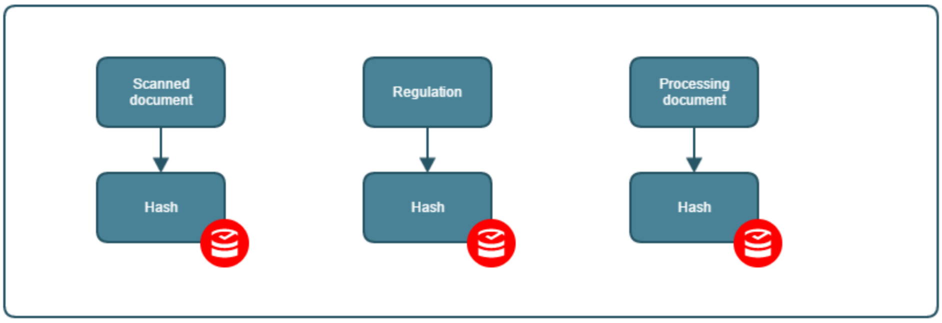


Figure 4: The KSI Blockchain in the Business Registry. Source: Ivo Lõhmus, Guardtime.

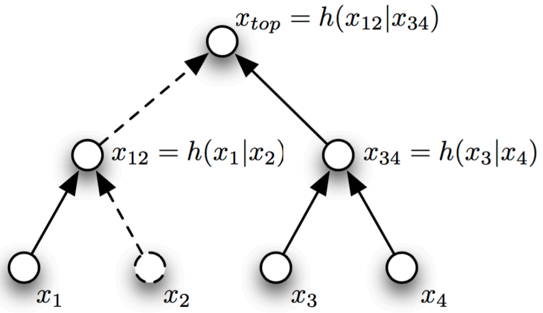
The Estonian e-Health Authority has implemented other innovative uses of blockchains. It has partnered with the systems engineering firm Guardtime to protect the integrity of more than one million heath records.[xxii] In this context, the application of blockchain technology will enable independent and 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 5 above).

In sum, following is a list of Estonian State Agencies that are currently implementing and utilising KSI blockchain technology within their respective service domains:

- 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

A Technical Overview of the Keyless Signatures Infrastructure (KSI)

What technical features underpin the KSI blockchain? The technology relies on Hash Trees (HT), a data structure that can be used to protect the integrity of documents using cryptographic hash functions. 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 7 below illustrates this procedure.



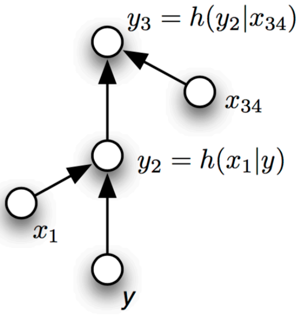


Figure 5: An example of a Hash Tree (left) as used in Keyless Signatures' Infrastructure. Hashes of the documents (x1–x4) are stored as leafs in the Hash Tree. The intermediate nodes are generated by hashes, which are computed over aggregated hashes from the layer below. The top hash (x_{top}) represents the overall Hash Tree. 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 hash tree and has not been modified.

Source: Ahto Buldas, Andres Kroonmaa, and Risto Laanoja, *Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees. 2013*.

In the case of KSI, a hash tree 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 hash tree. The top hashes from each round are linked together in a global hash tree called a hash calendar. The top hash of the calendar is periodically published and distributed on a hard-to-modify media, such as a newspaper.

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.[xxiii]

Aggregation Network

Aggregator network is 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 aggregator 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 hash tree. After receiving a response from an upstream component, an aggregator delivers the response to all child aggregators 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, KSI relies on redundancy: every aggregation server is made of a geographically dispersed cluster of aggregation servers.

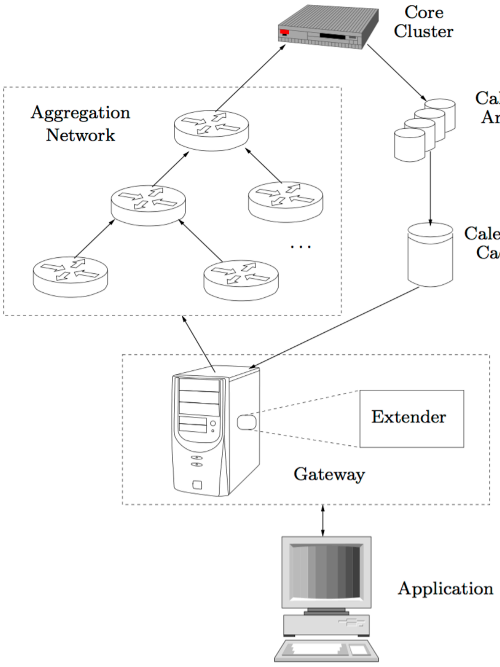


Figure 6: The main architecture of the KSI. The application performs the first hashing step, which also generates the signing request. The signing request is sent to the gateway, which forwards it to the aggregation network. The aggregators build the hash tree and pass the top hash values upstream. Once 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 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.***

Core Clusters

Core clusters are distributed synchronised 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 synchronisation, which represents the issuing time of each signature token.

The aggregation servers propagate their top hash values to all core nodes. A multi-party protocol is used to detect discrepancies in the submitted top hashes; only the values which are identical from the majority voting of core servers can be written in the calendar database.

KSI Gateways

The KSI gateways are protocol adapters: they serve as interfaces for different applications that use the KSI blockchain. The gateways also 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 trusted party.

KSI Blockchain: a discussion of security objectives

The main security objective provided by Estonia's use of KSI blockchain is data *integrity*. As discussed in Section 2, this involves guaranteeing that an unauthorised party has not modified information. 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.

Only the hashes are stored in the KSI blockchain. Thus, there is a preservation of data *privacy*, because the original document cannot be recreated from hashes. Such an approach, however, means that other security objectives discussed in Section 2 need to be provided. In the Estonian context, the overall system's security depends on the *authentication* and *confidentiality* protocols provided by both the X-Road and KSI authentication services.

Data Availability

The KSI blockchain stores cryptographic representations of data using one-way cryptographic hash functions. This means 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. 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 physically cloning data storage facilities. For instance, a *hot site* can replicate all the equipment and data while offering minimal recovery time. *Warm* and *cold sites* could provide different trade-offs between recovery time and costs in running such sites.

In general, a significant physical distance between the recovery sites is required to minimise the effect of catastrophic events. This requirement poses a problem for geographically small countries like Estonia. For this reason, Estonian authorities have developed the concept of Data Embassies, which involves the maintenance of hosting facilities outside of the national territory (yet within the government's legal jurisdiction).[xxiv] 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 blockchains. At present, the implementation of Data Embassies has just begun; several legal and technical challenges remain unsolved. But the concept offers an intriguing and promising approach to disaster recovery in support of blockchain technology.

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 (called the "trapdoor"). Trapdoor functions are the main building blocks of conventional asymmetric cryptography, such as RSA or Diffie Hellman (the main security mechanisms used in asymmetric cryptographic protocols and PKI-based systems). A recent study by Ahto Buldas, Risto Laanoja, and Ahto Truu describes the quantum-resilient properties of the KSI. [xxv] The authors discuss the case of quantum-computational attacks and its impact on the security of the KSI blockchain. The KSI's resilience to such attacks is claimed by avoiding the trapdoor functions and only using cryptographic hash functions and publication of the hashes as the KSI's main security mechanisms.

Use of Blockchain Technology in Other Countries

A recent report by the UK Government's Chief Scientific Advisor provides interesting case studies of integrating blockchain technology into governmental processes in the United Kingdom.[xxvi] 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. It is estimated that DWP, for example, pays around £166 billion of taxpayers' money in welfare support per year. Around £3.5 billion of that amount is overpaid through fraud, claimant errors, and official errors—an astonishing loss of public money.

Blockchain technology provides an alternative and potentially superior disbursement method: it enables end-users to receive benefits directly into their digital wallets. This method would also reduce the transaction costs to banks and local authorities, as well as helping 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 benefits.

Recently, Guardtime and Future Cities Catapult Partner (UK) announced a partnership to develop blockchain-based cybersecurity services for critical UK infrastructure. Future Cities Catapult, the UK-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 UK 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."[xxvii]

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:[xxviii]

- *Increase 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.
- *Increase the 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 to complete the transaction.
- *Decrease the 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 minimising 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.

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

Conclusion

The use of blockchain technologies in public life and governmental affairs offers notable 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 blockchain technology. The private sector is attracted to the efficiency and low cost. The centralised nature of traditional commerce does not scale well; the decentralised approach, in which information is shared, has conventionally been considered risky for businesses. Blockchain technology promises to resolve many of these issues. The technology is able to preserve the integrity and confidentiality of records stored within it using well-established cryptographic methods; at the same time, the distributed nature of blockchains enables different stakeholders to "own" it. Thus the 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 security guarantees provided by the overall system. 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 authorisation 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 in this paper, the public blockchains that are based on Proof-of-Work protocols have inherent "self-healing" properties based on a resource investment that the system rewards. By contrast, private blockchains such as Estonia's avoid these often energy-inefficient mechanisms. Private blockchains are optimised for specific application scenarios and rely on pre-existing 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 generalised. Their capabilities and resistance to strong adversaries depends on a concrete trust model and implemented security mechanisms, which are used to preserve trust and protect the peers from insider and outsider attacks.

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 include the following: How resilient is the consensus mechanism to various attacks? 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.

The author is thankful for the helpful insights and information that he received in technical interviews with Andres Kütt, Mikk Lellsaar, Ivo Lõhmus, and Kuldar Aas during the preparation of this paper.

References

[i] UK Chief Scientific Advisor, *Distributed Ledger Technology: 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.

[ii] 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.

[iii] Philip Boucher, "What If Blockchain Technology Revolutionised Voting?" *What If…?* Scientific Foresight Unit (STOA), European Parliament Research Service, September 2016.

[iv] See Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review."

[v] 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.

[vi] See "Blockchain," *e-Estonia Showroom*, https://e-estonia.com/tag/blockchain/; and "Blockchain-Enabled Cloud: Estonian Government selects Ericsson, Apcera and Guardtime," *Guardtime*, https://guardtime.com/blog/blockchain-enabled-cloud-estonian-government-selects-ericsson-apcera-and-guardtime.

[vii] A good summary can be found in Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *The Handbook of Applied Crypto* (city and state/country of publication?: CRC Press, 1996).

[viii] For a good summary, see Anthony Lewis, *A Gentle Introduction to Blockchain Technology*, BraveNewCoin.

[ix] This example is taken from Lewis, *A Gentle Introduction to Blockchain Technology*.

[x] The longest-chain rule is more important than just a 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. For more on this point, see the next section.

[xi] See Ethan Heilman and Alison Kendler, "Eclipse Attacks on Bitcoin's Peer-to-Peer Network," *Usenix Security,* 15 (August 2015).

[xii] Lear Bahack, "Theoretical Bitcoin Attacks with less than Half of the Computational Power," arXiv:1312.7013 [cs.CR.].

[xiii] 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*, pp. 57–71.

[xiv] 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, our 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/.

[xv] See ibid.

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

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

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

[xix] See Enterprise Estonia, "X-Road," *e-Estonia.com: The Digital Society*, https://e-estonia.com/component/x-road/.

[xx] See Cybernetica, "X-Road," https://cyber.ee/en/e-government/x-road/.

[xxi] See Enterprise Estonia, "X-Road."

[xxii] 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.

[xxiii] 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.*

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

[xxv] 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,* 08/23, 2017.

[xxvi] See UK Chief Scientific Advisor, *Distributed Ledger Technology*.

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

[xxviii] See The Swedish Mapping, Cadastre and Land Registration Authority, Telia, ChromaWay, and Kairos Future, “The Land Registry in the Blockchain: A Development Project with Lantmäteriet,”, Sweden July 2015.