Science and Technology Trends
Blockchain Industries, Regulations and Policy

Blockchain Industry, Regulations and Policy in Estonia

Risto Hansen

1. Introduction − blockchain trends in Estonia, the leading country in the blockchain industry

While named 'the most advanced digital society in the world' by Wired (Hammersley, 2017), Estonia is a true pathfinder in e-governance solutions. The Baltic state has built an efficient, secure and transparent ecosystem, saving its population, as well as the public system, both time and money. About two decades ago, when the information society was starting to develop in Estonia, no digital data on Estonian citizens was being collected. The general population did not have access to the Internet or even devices enabling access to it. It took a great deal of courage from the Estonian state to invest in information technology (IT) solutions and take the first innovative steps down the information technology road, steps which have now transformed Estonia into one of the world's most developed digital societies.

However, being a digital society also means exposing oneself to cyber threats. After Estonia's experience with the 2007 cyber-attacks (e.g. Ottis, 2018), scalable blockchain technology was developed to ensure the integrity of data stored in government repositories and to protect this data against insider threats. With KSI Blockchain, deployed in the Estonian government networks, history cannot be rewritten by anybody and the authenticity of electronic data can be mathematically proven. It means that no-one − not hackers, not system administrators, and not even the government itself − can manipulate the data and get away with it.

With the fourth industrial revolution, the importance of fostering blockchain industries is becoming more apparent. Solid investments in cyber security infrastructure have helped Estonia develop extensive expertise in this area, becoming one of the most recognised and valued sources of international cybersecurity expertise. Today, Estonia is host to the NATO Cooperative Cyber Defence Centre of Excellence and the EU-LISA (the European Union IT agency), showcasing the strategic focus of the country's innovation, research and development within the spheres of cyber security and cyber defence and domestic and international cyber defence exercises and trainings. Also offering reliable day-to-day management of the related infrastructure, hosting large, critically valued, EU databases.

Technology changes rapidly, this is also true in the blockchain industry. It is important to understand the nature, benefits and use-cases of blockchain technology as much as to consider its misconceptions

Head of eGovernment Solutions, Guardtime, A. H. Tammsaare tee 60, Tallinn, 11316 Estonia
E-mail: ristohansen@gmail.com

and future challenges, impacting wider implementation and development within the industry.

2. Understanding the background of blockchain in Estonia

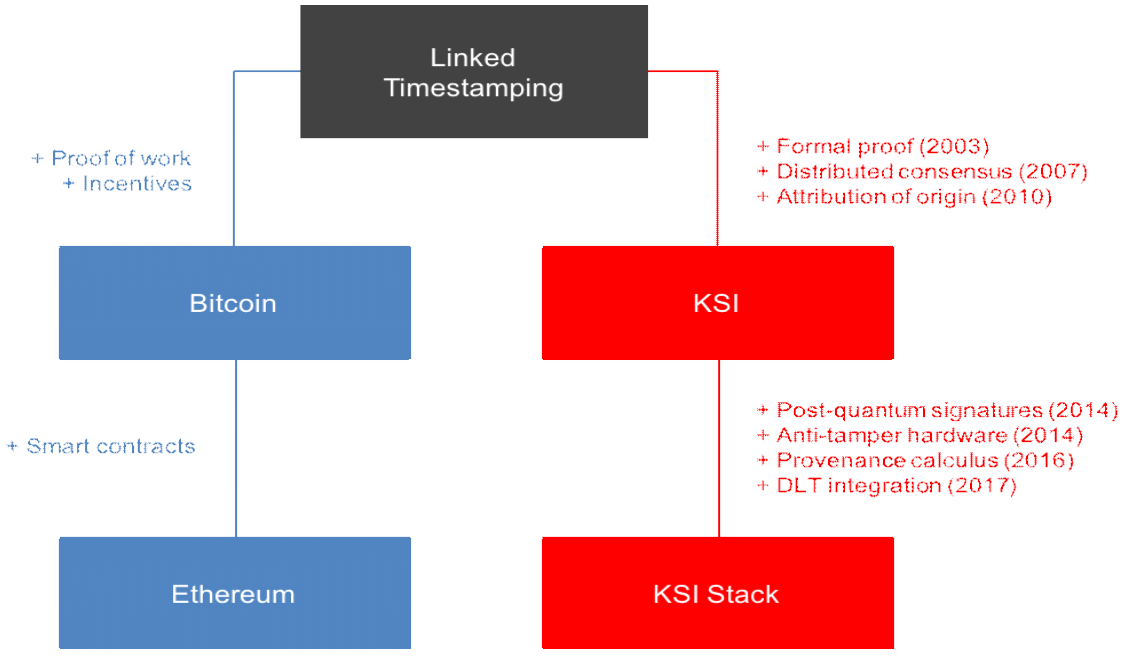
After taking the first steps toward becoming an e-state, Estonia realised that the risk of cyber-attacks will always be part of the information society – a risk that must be taken seriously. After analysing different options, Estonia found a solution for this: blockchain technology – a mathematically ensured cyber security solution for identifying the use and misuse of digital data and intelligent devices, providing transparency and reliability to all organisations and institutions related to and working with digital data or intelligent devices in the public or private sector.

Although blockchain has only become 'hot' technology in recent years, Estonia is leading the way in the blockchain revolution – the state has been testing the technology since 2008, i.e. even before the release of the Bitcoin whitepaper which first coined the term "blockchain" (Nakamoto, 2008). Since 2012, blockchain has been employed in Estonia's data registries, such as the national health, judicial, legislative, security and commercial code systems, with plans to extend its use to other spheres such as personalised medicine, cyber security and data embassies.

2.1. From timestamping to the blockchain

While the academic pedigree of bitcoin often goes unknown, the cryptography behind those individual components has been well known since the 1990s (Haber & Stornetta, 1991) and Guardtime's cryptographers have been very active participants in that history.

Figure 1. Blockchain Technology Family Tree



Source: Guardtime (2018a)

One of the core concepts behind bitcoin is called 'linked timestamping' and Professor Ahto Buldas and Märt Saarepera (PhD) of Guardtime were the first cryptographers to give a formal security proof in 2003, i.e. defining what properties are needed for hash-functions and data structures in order to build a formally verifiable security proof (Buldas & Saarepera, 2004).

Formal verification might sound arcane but if you want to build a house you had better make sure the foundations are solid – and formal methods and verification are the basis of everything that Guardtime does today.

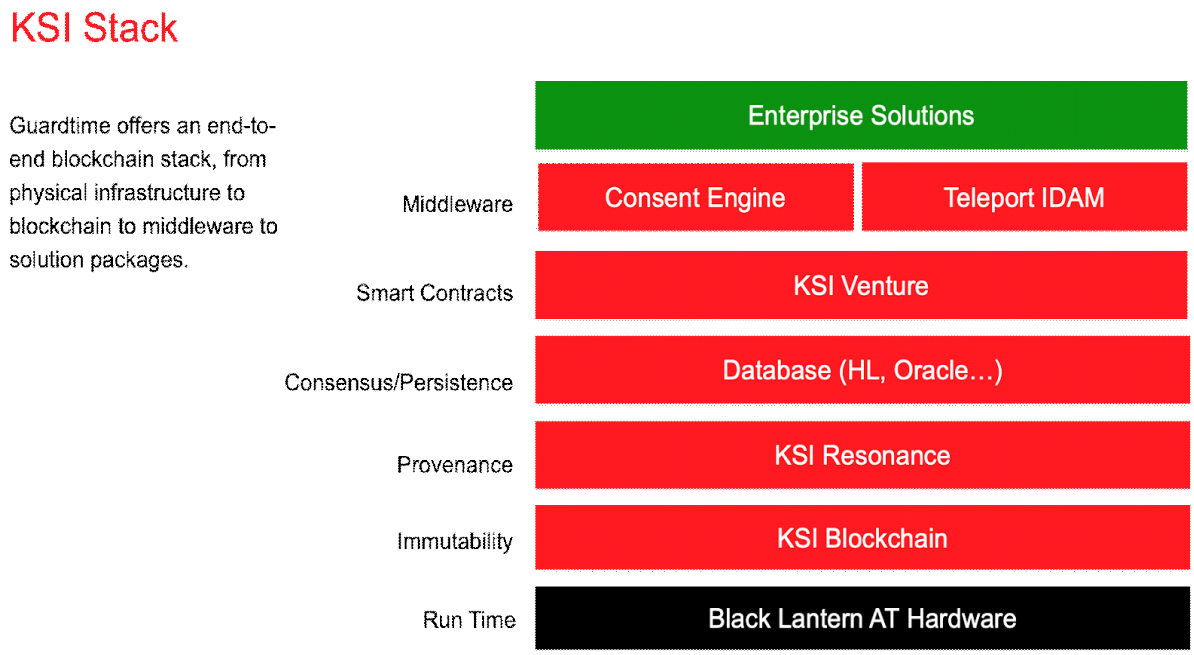
The Estonian blockchain company Guardtime was launched in 2007 with the goal of creating a formally verifiable security system for the Estonian Government, i.e. eliminating third parties, trusted insiders or cryptographic keys in the verification of the integrity of government records, networks and systems.

Cryptography, like mathematics, starts off with assumptions (axioms) and derives conclusions from those assumptions. The goal was to eliminate humans from the list of assumptions needed to make assertions about the time and integrity of digital records, such as documents in a government registry, configuration files in a network router, or software running inside an IOT device, etc.

The challenge was not cryptography but engineering, building a scalable and reliable service for the government that would continue to function even under constant cyber-attack.

As a result, the system was successful and went into production in April 2008 and over the last decade, Guardtime has continued to innovate, adding more and more functionality to the platform. Guardtime has added post-quantum signatures to replace RSA, Anti-Tamper hardware (Black Lantern), a provenance calculus designed to track and trace digital information as it crosses organisational boundaries and many other new features (Guardtime, 2018a).

Figure 2. Guardtime's KSI ® Technology Stack



Source: Guardtime (2018)

The result is a stack of technologies, designed in the spirit of the Unix philosophy – abstraction and encapsulation of functionality into layers, each of which does one thing well.

Ultimately blockchains are just tools used to solve customer problems. Guardtime's mission is to leverage these tools, work with partners and build the highest-quality enterprise solutions possible.

2.2. Estonian KSI Blockchain Technology

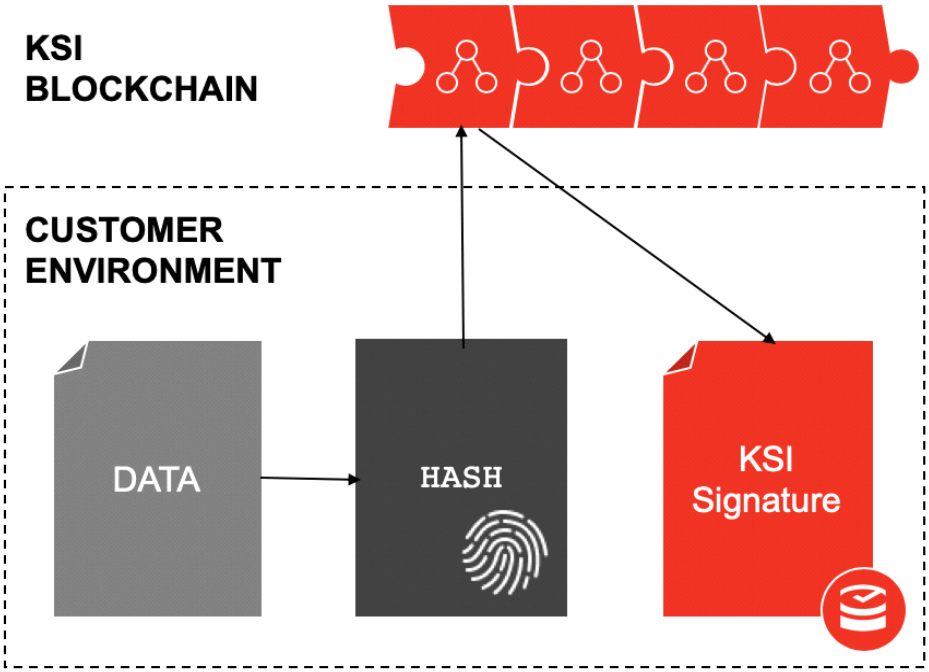
KSI Blockchain technology, developed by Guardtime, is designed in Estonia and used globally to ensure networks, systems and data are free from compromise, all while retaining 100% data privacy. Today, KSI blockchain is available in several countries, while scaling 1012 items of data every second globally.

By its nature, it is a mathematically assured cybersecurity solution for detecting the use and misuse of digital data and devices. The KSI Blockchain is a globally distributed network infrastructure and method for issuing and verifying KSI signatures.

Unlike traditional digital signature approaches, e.g. Public Key Infrastructure (PKI), which depend on asymmetric key cryptography, KSI uses hash-function cryptography only, allowing verification to rely only on the security of hash functions and the availability of a public ledger – commonly referred to as a blockchain (Guardtime, 2018). A blockchain is a distributed public record of events; an append-only record of events where each new event is cryptographically linked to the previous. New entries are created using a distributed consensus protocol (ibid).

A user interacts with the KSI system by submitting a hash-value of the data to be signed into the KSI infrastructure and is then returned a signature which provides cryptographic proof of the time of signature, the integrity of the signed data, as well as attribution of origin, i.e. which entity generated the signature.

Figure 3. KSI Blockchain and Customer Environment



Source: Guardtime (2018)

The benefits of the KSI include (Guardtime Federal, 2018):

- Massive Scale. KSI signatures can be generated at exabyte-scale. Even if an exabyte (1,000 petabytes) of data is generated around the planet every second, every data record (a trillion records assuming 1MB average size) can be signed using KSI with negligible computational, storage and network overheads.

- Portability. The properties of the signed data can be verified even after that data has crossed geographic or organisational boundaries and service providers.

- Data Privacy. KSI does not ingest any customer data; data never leaves the customer premises. Instead, the system is based on one-way cryptographic hash functions that result in hash values uniquely representing the data. These are irreversible, such that one cannot start with the hash value and reconstruct the data − data privacy is guaranteed at all times.

- Independent Verification. The properties of the signed data can be verified without reliance or need for a trusted authority.

3. Blockchain in Estonia Today

While using KSI blockchain with many registries, today Estonia uses a variety of innovative solutions that have been developed for the Estonian government. Siim Sikkut, Estonian Government CIO, Ministry of Economic Affairs − has brought out that the goal of Estonia using blockchain is to increase citizens' trust in public services by ensuring data integrity (Si-soo, 2018). Therefore, the government is continuing to carry out various experiments with blockchain to test how much it can support the existing system of the Estonian e-state and expand its implementation.

3.1. Various use-cases

For example, in Estonia blockchain technology helps to detect who looks at a person's digital health data, who changes it and when. In order to keep health information completely secure and, at the same time, accessible to authorised individuals, the electronic ID-card system is used.

The Estonian e-Health Record[1] uses blockchain technology to ensure data integrity and mitigate internal threats to the data. The main value that blockchain provides is immutability of the logged activities, ensuring that neither adversaries nor insiders could tamper with the data nor cover up the tracks of malicious activities. As a result, every occurrence of data use and misuse is detectable and major damages to a person's health can be prevented (such as a prescription for the wrong medicine or an incorrect dose).

Another example of Estonian blockchain integration is the Estonian National Gazette[2], where maintaining data integrity is extremely vital. Since 1 June 2010, the electronic National Gazette has been the one and only publication where laws and regulations are published. The whole of Estonia relies on the information provided by the National Gazette. There is no paper copy to turn to if something is wrong in the portal. What you can see in the National Gazette is what the law has been and currently is in Estonia. To protect such an important database, the Estonian Centre of Registers and Information Systems uses various security measures, one of them being the KSI Blockchain.

1) See: The Patient Portal: https://www.digilugu.ee/login?locale=en
2) See: State Gazette: https://www.rik.ee/en/international/state-gazette

Besides these examples, the Estonian KSI Blockchain technology protects a number of other Estonian e-services, such as the e-Prescription database, e-Law and e-Court systems, e-Police data, e-Banking, the e-Business Register and the e-Land Registry. For example, it can help to see when information about a company in the Estonian e-Business Register was changed and why; or to detect who changed data about a real estate property in the Estonian e-Land register; or statements documented in the e-Court system, as well as when and how these were changed.

3.2. Deploying blockchain in Estonia

In order to deploy blockchain in Estonia's state information systems, the Estonian Information Systems Authority (RIA), as an internal service provider for the government, guarantees access to the blockchain network for state agencies via the X-Road infrastructure (e-estonia.com, 2018). The Estonian state agencies deploy blockchain technology by themselves, using the Software Development Kits (SDKs) and prebuilt tools, i.e. for log and database integration.

However, according to Mehis Sihvart, Director of the Centre of Registers and Information Systems (RIK), it still often comes as a surprise to hear that most of the government registers in Estonia today are operated electronically (Sihvart, 2017). While the key question here is to guarantee integrity and safety, the Estonian government and RIK have found blockchain to be a tried, tested and suitable technological method for guaranteeing the integrity of government data.

Sihvart explains that RIK, which is currently managing and administrating over 70 information systems and registers in Estonia, started implementing blockchain first for its Register of Wills/Succession Registry in 2012. According to the initial idea, RIK takes will information from the database and anchors it to the blockchain so that no one can remove or change the will in the registry. The information sent to the blockchain is encrypted while RIK validates the data against the blockchain, and therefore knows the data has not been removed or tampered with. According to Sihvart, this gives a good level of security when managing this as well as other government registers (ibid).

In fact, the same KSI Blockchain technology described above is used globally in many sectors. A few notable defence and commercial implementations include Verizon, Ericsson, Lockheed Martin, Maersk, DARPA, Ericsson, EY, etc (Guardtime, 2018b).

4. Myths and Legends About Blockchain in Estonia

There are several myths and misconceptions related to blockchain in Estonia, which must be corrected. Let us review them.

First, it is often misunderstood that the data of the Estonian population is stored on the blockchain and that the main database structure in Estonia is based on the blockchain platform. This is untrue, as there is no personal data on the blockchain – there is no need for it. The only digital fingerprints, i.e. hashes, of data are put to the blockchain for integrity assurance.

Another misconception concerns IDs based on the blockchain. It has been brought out that Estonia has been operating a universal national digital identity scheme using blockchain, but this fact is incorrect. The blockchain is not used for IDs. Instead, Estonia has a national PKI infrastructure for that – blockchain is used within registries/systems for integrity purposes. However – R&D on quantum immune, blockchain backed IDs – is ongoing and therefore we might not know the possibilities that are to come in the future.

The third blockchain myth in Estonia is the statement that the X-Road is a blockchain based technology or it utilises blockchain internally. Actually, the X-Road is not a blockchain and it does not use blockchain today. The X-Road is the secure data-exchange layer which is used to connect the registries and services in Estonia. However, blockchain service (for integrity assurance) is one of the services available on the Estonian X-Road. The X-Road itself is just a transport layer which facilitates blockchain access.

These kinds of misconceptions include several other false ideas, such as the statement that bitcoin and blockchain consume an exorbitant amount of energy or that one bitcoin transaction uses as much energy as one's house in a week. However – this all applies to public blockchain technology (Proof of Work (PoW) based) only, while PoW is needed when participants are anonymous. As Estonia uses permissioned blockchain technology, participants are known and there is no need for PoW.

5. Global Use-Cases of KSI Technology

It is important to understand and to continue developing and implementing blockchain technology solutions into the financial sector or state institutions and in other fields of businesses in order to introduce their potential and benefits more widely. Different fields around the world are expected to combine their solutions with blockchain technology, and here Estonia can certainly share its experience. In the section below, a number of successful use-cases of KSI technology are examined.

5.1. PRIViLEDGE

Although based on cryptographic techniques at their core, the currently deployed blockchain and distributed ledger technologies (DLTs) have privacy challenges. Indeed, the very idea of a public ledger that stores a verifiable record of transactions at first appears inherently incompatible with the privacy requirements of many potential applications, which use sensitive data, such as trade secrets and personal information. New cryptographic techniques and protocols are therefore needed to protect the data, facilitate these applications, and make DLTs deliver on their promises (Priviledge, 2018).

PRIViLEDGE, as a consortium of 10 EU organisations, realises cryptographic protocols supporting privacy, anonymity, and efficient decentralised consensus for DLTs. Within this EU-funded project, several key European players in cryptographic research and from the fintech and blockchain domains, including Guardtime, unite to push the limits of cryptographic protocols for privacy and security. Results from PRIViLEDGE are demonstrated through four ledger-based solutions: verifiable online voting, contract validation and execution for insurance, a university diploma record ledger, and an update mechanism for stake-based ledgers (ibid). The selected use cases are diverse and represent the principal application domains of DLT while ensuring a wide reach and impact of the techniques developed in PRIViLEDGE beyond the immediate scope of the project.

5.2. SOFIE

Another example here is the SOFIE project, which aims to develop a blockchain driven federated platform for enabling information exchange of numerous Internet of Things (IoT) and data silos (Sofie, 2018). The goal of this EU-project is to enable the creation of business platforms, based on existing IoT platforms and distributed ledgers, without needing to negotiate with any gatekeepers.

The wide applicability of the approach of the SOFIE project is tested through four pilots. Within that, Guardtime is implementing an energy pilot,

which will demonstrate how the SOFIE federated framework can be used for providing reliable data feeds and exchange power consumption information among energy grid participants, in order to allow flexible services based on smart meter data (ibid).

5.3. Insurwave

The blockchain is now also applied to the world's first platform for marine insurance in commercial use. In spring 2018, Guardtime, EY and other partners announced the blockchain platform Insurwave, which helps global businesses to transform the management of risk and the way of working with brokers and (re)insurers across the organisations (Guardtime, 2018c).

Insurwave leverages blockchain and distributed ledger technologies while supporting more than half a million automated ledger transactions and helping manage risk for more than 1,000 commercial vessels in its first year. By connecting participants in a secure, private network with an accurate, immutable audit trail and services to execute processes, the platform establishes a first of its kind digital insurance value chain (ibid).

6. Future challenges

With rapid changes in technology the blockchain industry will remain in constant development and must respond to the demands coming from the surrounding environment. Among other aspects, new standards for digital identity and blockchain, as well as novel technologies, such as artificial intelligence (AI), will need to be considered.

6.1. New quantum-immune blockchain standard for digital identity

In May 2015, Guardtime announced BLT, the authentication and signature protocol meant to replace RSA as the standard for digital identity (Guardtime, 2018d). In contrast to RSA's reliance on quantum-vulnerable asymmetric key cryptography, BLT is based on Guardtime's quantum-secure KSI technology, which uses hash function cryptography only.

Mike Gault, CEO of Guardtime explained then (ibid) that the RSA has been dominating the digital signature scheme since the 1970s, but it is outdated and cannot scale for the explosion of data or devices we are seeing with the Internet of Things, mobile and machine-to-machine technologies. Most importantly, on the advent of quantum computers, RSA could be rendered completely useless. No practical and scalable alternative for the market existed, until BLT, which provides a scalable, secure alternative to RSA – practical for authenticating not only data in motion, but also for data at rest in the cloud or as part of the infrastructure.

As KSI blockchain technology employs one-way hash functions to generate digital signatures that can prove the time, integrity and attribution of origin for electronic data, BLT extends this approach to provide human and machine identity management, with a level of non-repudiation consistent with existing digital signature schemes.

Through this methodology, BLT offers simplified revocation management: there is no need to check the certificate validity when verifying signatures, eliminating the need for complicated Certificate Revocation Lists (CRLs). It also benefits via long-term validity: there is no need for periodic re-timestamping of the signatures due to expiring keys – the time and integrity of the signature can be proven mathematically, without reliance on trusted parties or the security of the keys.

Unlike RSA, BLT signatures cannot be generated offline, removing the potential for unlimited liability in the case of private key theft. Also, BLT's hash functions cannot be broken using quantum

algorithms.

Matt Johnson, CTO of Guardtime has stated (ibid) that, apart from robust security, e-commerce and/or device registration applications, BLT greatly improves the strength of any signing and authentication process.

As a result, BLT collapses security issues and removes traditional trust anchors with this new signature scheme. It's clean, efficient and beautifully simple, demonstrating the power of KSI to transform the world's security landscape.

6.2. "Kratt law" to legalise Artificial Intelligence (AI) in Estonia

Another future challenge within the blockchain industry is strongly related to the fact that countries around the world are facing the challenge of understanding the rise of AI, which is increasingly affecting the daily lives of people all over the world. This raises the question: which country will be the first in developing a comprehensive legal framework that ensures that the technology can be developed in an ethical and sustainable way?

Marten Kaevats, National Digital Advisor for The Government Office of Estonia, has stated that while Estonia is known for its "firsts" – as the first country to declare internet access as a human right, the first country to hold a nationwide election online, the first country in Europe to both legalise ride sharing and delivery bots, and the first country to offer e-Residency – Estonia should be the first to develop this legal framework also (Kaevats, 2017).

The work to understand AI in Estonia started in November 2016, with the self-driving vehicles task force, together with the Estonian Ministry of Economic Affairs and Communications and the Government Office. However, it quickly became clear that their scope was too limited, as working on traffic regulations is simply not enough given the far-reaching implications of the technology. As a result, the task force suggested four different options regarding how to regulate AI in a user-friendly way.

According to Kaevats (ibid), within this process, the Estonian government authorities have acknowledged that the biggest obstacle for mass implementation of AI is our current cyber capabilities, particularly regarding, firstly, the integrity of these systems and, secondly, their security. Similar to life and death decisions made by self-driving cars, it is important to be sure that the decision-making algorithm has not been tampered with.

Today, Estonia has recognised the complexity, scope and possibilities of these issues and aims to contribute to the global discussion with positive case studies with an emphasis on ethics and cyber measures. The immense possibilities of AI cannot be enabled if there are no right values and right regulations.

However, from a governmental perspective, it is also crucial to consider the practical enforcement side of implementing these kinds of measures as well. Therefore, the Estonian government is working together with Guardtime to ensure measures of anti-tampering and data integrity within these AI algorithms.

7. Conclusions

Successful countries need to be ready to experiment. Building e-Estonia – one of the most advanced e-societies in the world – has involved continuous experimentation and learning from mistakes.

Increasing levels of cybercrime and politically motivated attacks on data, as well as electronic services, show that cyber security is more important than ever for the private and public sector, and citizens alike. Estonia's preparedness to handle cyber crises has significantly increased over the past decade. The

country has created intrusion detection and protection systems, practiced cooperation with both public and private institutions, significantly contributed to the awareness of users, and is participating in intensive international cooperation.

After its experience with the 2007 cyber-attacks, Estonia has implemented blockchain technology to ensure data and system integrity and combat insider risk and has become a powerhouse of cybersecurity expertise. Estonia uses Guardtime's KSI Blockchain technology, which is purpose-built for mass-scale integrity verification. Based on original academic research, it predates even Bitcoin and has been used in production for more than 10 years. Contrary to the common understanding that blockchain is used to store transactions, the KSI Blockchain only ingests cryptographic hash values, therefore, it is 100% privacy preserving and complies with all regulations.

KSI Blockchain technology was created in Estonia but has now taken off on a global scale. Guardtime can be considered the world's largest commercial blockchain technology provider, with implementations in the public sector, defence, healthcare, and many more.

Estonia is ready to share its experiences and lessons openly with the whole world. Through rapid reforms, creating new solutions and being a role model to the world, it is inevitable that sometimes things go wrong. However, it is important to stick to one's principles, learn from one's mistakes and to talk openly about them. A key feature of a true expert is having the courage to talk about their mistakes – this is exactly how Estonia has managed to build such a successful digital society.

References

Buldas, A. & Saarepera, M. (2014). On provably secure time-stamping schemes. <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.65.8638>

e-estonia.com. (2018). Frequently asked questions: KSI Blockchain in Estonia. <https://e-estonia.com/wp-content/uploads/faq-ksi-blockchain-1.pdf>

Guardtime. (2018a). KSI Technology Stack. <https://guardtime.com/technology>

Guardtime. (2018b). <www.guardtime.com>

Guardtime. (2018c). World's first blockchain platform for marine insurance now in commercial use. <https://guardtime.com/blog/world-s-first-blockchain-platform-for-marine-insurance-now-in-commercial-use>

Guardtime. (2018d). BLT new blockchain standard for digital identity. <https://guardtime.com/blog/blt-new-blockchain-standard-for-digital-identity>

Guardtime Federal. (2018). What is Keyless Signature Infrastructure (KSI). <https://www.guardtime-federal.com/ksi/>

Haber, S. & Stornetta, W. S. (1991). How to time-stamp a digital document. Journal of Cryptology archive, 3(2), pp 99-111 <https://www.anf.es/pdf/Haber_Stornetta.pdf>

Hammersley, B. (2017). Concerned about Brexit? Why not become an e-resident of Estonia. <https://www.wired.co.uk/article/estonia-e-resident>

Kaevats, M. (2017). Estonia considers a 'kratt law' to legalise Artifical Intelligence (AI). <https://medium.com/e-residency-blog/estonia-starts-public-discussion-legalising-ai-166cb8e34596>

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, 2008. Reading: Academic Publishing Limited, pp 163-168. https://www.etis.ee/File/DownloadPublic/b924739a-01f6-4867-8e86-1d4527c22e31?name=Fail_2008_ECIW_Ottis.pdf&type=application%2Fpdf

Priviledge. (2018). About. <https://priviledge-project.eu/about>

The Patient Portal. (2018). Patient Portal. <https://www.digilugu.ee/login?locale=en>

Si-soo, P. (2018). Blockchain is not a silver bullet. The Korea Times. <http://m.koreatimes.co.kr/pages/article.asp?newsIdx=251980>

Sihvart. (2017). Blockchain – security control for government registers. <https://e-estonia.com/blockchain-security-control-for-government-registers/>

Sofie. (2018). Secure Open Federation for Internet Everywhere. <https://www.sofie-iot.eu/>

State Gazette. (2018). State Gazette. <https://www.rik.ee/en/international/state-gazette>