FREQUENTLY ASKED QUESTIONS

Estonian blockchain technology

What is blockchain technology and how is it related to e-Estonia?

Blockchain is a mathematically ensured cyber security technology for rapid and immutable identification of modifications in digital data and intelligent devices. Blockchain technology makes it possible to discover any and all changes made to digital data, no matter how small, no matter by whom, immediately and with zero error.

Although blockchain has only become hot topic in recent years, Estonia started testing the technology already in 2008 — even before the Bitcoin white-paper that first coined the term "blockchain", was published. At that time, in Estonia we were calling this technology "hash-linked time-stamping". Since 2012, blockchain has been in production use in Estonia to protect national data, e-services and smart devices both in the public and private sector.

How does blockchain work?

One way to look at the blockchain technology is to view it as a "digital defence dust" that covers all the data and smart devices that need to be protected from corruption and misuse.

- Every change in data can be instantly detected based on traces left in the pattern of the "digital defence dust" that covers the data
- Blocks of "digital defence dust" are connected to each other and make up a chain that is distributed in millions of computers all over the word, which makes it impossible to change data so that nobody knows — the chain instantly reflects all changes that mismatch the mathematical code in the chain

This way millions of lives and resources are saved, while the potential manipulation of sensitive data (such as health data, intelligence information, legislation-related records, etc.) or smart devices (such as military machinery, hospital equipment, intelligent cars etc.) is prevented or instantly detected.

One can compare the idea of the blockchain to the NATO allies in Estonia — while the NATO allies are not actively holding back invaders on a daily basis, they are most certainly acting as a deterrent against any potential threats.

How is blockchain used in e-Estonia?

Although blockchain has only become hot technology in recent years, Estonia has been testing the blockchain technology since 2008. Since 2012, blockchain has been in production use 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 personal medicine, cyber-security and data embassies.

Why should blockchain technology be trusted?

No data is ever stored on a Blockchain - instead blockchain works like a speed camera that detects who has violated the law, when and how. Due to the fact that data, protected by blockchain technology, is covered with the "digital defence dust", every change in the data can be detected because it leaves a trace in the pattern.

The particular blockchain technology used by Estonia — KSI Blockchain by Guardtime — has been proven to work and is today even used by NATO and US Department of Defense.

European Union
European Regional
Development Fund

Investing
in your future

What makes blockchain technology so special?

The blockchain technology used in Estonia is different from mainstream blockchains due to its scalability. This means that even large amounts of data can be covered with "digital defence dust", since the parts of the dust (blocks) are connected to each other using a mathematically verifiable code that connects the blocks into a chain, which cannot be changed without leaving a trace behind.

What is the difference between blockchain and Bitcoin?

"Blockchain" and "Bitcoin" are two separate terms and should not be confused. While blockchain is a technological concept, Bitcoin is one of the use cases for a particular type of a blockchain technology. Estonian government started testing blockchain technology for ensuring the integrity of the government e-services in 2008 — 6 months before Bitcoin was launched as a type of unregulated digital currency.

It is important to keep in mind that even though both, Estonian public e-services and international unregulated digital currencies such as Bitcoin are covered with "digital defence dust", the value of the digital currency may vary (increase or decrease), whereas the value of the data covered with "digital defence dust" does not change and this very fact makes the data even more valuable.

Who controls blockchain?

The chain of blocks of "digital defence dust" (aka blockchain) reaches a great number of computers all over the world, and can therefore be controlled and verified by great number of parties. The blockchain is, after all, just an internet-hosted network which stores information as a shared database. That means the information isn't stored in a single location and no centralised version exists for a hacker to corrupt, making it safe to use.

Some blockchain vendors - like Guardtime, a company behind the KSI blockchain used by Estonia - have gone even beyond that, and publish the blockchain also in the physical media, like the Financial Times newspaper. If someone would want to manipulate the KSI blockchain without anyone noticing, they would not only have to deal with the "digital defence dust" in the electronic domain, but also replace tens of thousands of copies of newspapers in the world's libraries. It is clear that no-one - not even Guardtime itself - is able to do that, and therefore the data on the blockchain can be considered immutable.

As a result, while it today takes on average about 7 months to discover the breach or misuse of an organisation's data, the blockchain helps to discover such threats instantly. For example, cases like Snowden would never have happened if the NSA had been using blockchain technology like in Estonia. It is important to point out that although blockchain may not prevent the crime itself, it is 100% effective in detecting it.

Blockchain-based cryptomoney frauds are common. So how can a state trust and use blockchain to protect the private data of its citizens?

When dealing with any sensitive data, it is obvious that this data should not be kept on the blockchain - after all, blockchain relies on a large number of eyes to keep it secure! Instead, in order to secure sensitive data, what is kept on the blockchain are the "hash values" - essentially digital fingerprints of the original data. Just like your own fingerprints uniquely represent you, but don't tell anything about your race, eye color or thoughts, the same applies to digital fingerprints - while uniquely representing the original data, it is impossible to know anything about the data itself based on the "hash values". Therefore - it does not matter if anyone gets their hands on the blockchain - there is absolutely no original data there to be compromised!

European Union
European Regional
Development Fund

Investing
in your future

Can you provide any examples of blockchain technology actually being useful in protecting important the data of some state or important company?

- Millions of lives and resources are saved as the potential manipulation of defence data or smart war machines is prevented using blockchain technology.
- In order to keep health information completely secure and at the same time accessible to authorised individuals, the electronic ID-card system used by the Estonian e-Health Record uses blockchain technology to ensure data integrity and mitigate internal threats to the data. In this way every occurrence of data use and misuse is detectable and major damages to a person's health can be prevented (such as the wrong medicine or the wrong dose).
- The Estonian KSI Blockchain technology protects Estonian e-services such as the e-Health Record, e-Prescription database, e-Law and e-Court systems, e-Police data, e-Banking , e-Business Register and e-Land Registry.
- The same KSI Blockchain technology is used by the NATO Cooperative Cyber Defence Centre of Excellence, European Union IT Agency, US Defence Department and also by Lockheed Martin, Ericsson and others.

What happens if a blockchain company goes bankrupt, how is data protection assured then?

The company itself can NEVER see the actual data that is protected, it only provides the "digital defence dust" solution that can ensure its integrity and mitigate internal threats. So nothing happens when a blockchain company disappears, all the data protected will remain verifiable for its integrity for forever based on the shared blockchain, and if applicable for a particular blockchain technology, also based on the physical publication of the blockchain in the world's newspapers.

How does blockchain technology contribute to the well-being of a layman?

Blockchain technology helps to ensure that data concerning the person is not misused.

For example:

- blockchain technology helps detect who looks at a person's digital health data and changes it and when;
- blockchain technology helps to see when information about a company in the e-Business Register was changed and why;
- blockchain technology helps to detect who changed data about real estate in the e-Land register or statements documented in the e-Court system as well as when and how;
- blockchain technology helps to ensure that no one has manipulated smart devices such as intelligent transportation or smart war machines that could become life-threatening.

How quickly can the misuse of data be detected using blockchain technology?

According to the research by FireEye, one of the leading cyber security vendors in the world today, it currently takes organizations on average of about 7 months to detect breaches and manipulations of electronic data.

With blockchain solution like the one Estonia is using, these breaches and manipulations can be detected immediately.

European Union
European Regional
Development Fund

Investing
in your future