Estonian blockchain technology

After the first steps towards becoming an e-state, Estonia understood that the risk of cyber attacks will always be part of the information society — a risk that must be taken seriously. After analysing different solutions, Estonia found a solution for this: blockchain technology.

Blockchain technology is a mathematically ensured cyber security solution for identifying use and misuse of digital data and intelligent devices, while providing transparency and reliability to all organizations 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 — Estonia has been testing the technology since 2008. Since 2012, blockchain has been in 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.

Securing NATO and EU

After Estonia's experience with the 2007 cyber attacks, scalable blockchain technology was developed by the Estonian blockchain company Guardtime.

Thanks to its mathematically verifiable code, which is distributed to millions of computers all over the world, blockchain technology can be seen as “digital defence dust”. It is “spread” over data and smart devices in the defence sector in order to detect every sign of the misuse of the data, according to changes in the “pattern of the dust”. In this way millions of lives and resources are saved, while the potential manipulation of defence data or war machines is prevented.

Thanks to its experience, Estonia is today home to the NATO Cooperative Cyber Defence Centre of Excellence and the EU IT-Agency that all use the Estonian KSI Blockchain technology to secure their systems.

Personal data under control

In contrast to everywhere else in the world, in Estonia, patients own their personal health data, which is secured by blockchain technology.

Since 2008, hospitals and doctors in Estonia are required to digitalise data and make it available in the e-Health Record. In order to keep health information completely secure and at the same time accessible to authorised individuals, the electronic ID-card system uses blockchain technology to ensure data integrity and mitigate the 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.

Questions & answers

How secure is blockchain technology?

Blockchain technology itself does not secure the data, but 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 digital defence dust that covers millions of computers all over the world, every use and misuse of the data can be detected, as it leaves a trace in the pattern. Thanks to implementing this technology, the situations that Mr Snowden caused would never happen in Estonia.

How is Estonian blockchain technology different from other similar technologies?

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 with a mathematically verifiable code that connects the blocks into a chain, which cannot be changed without leaving a trace behind.

Facts and figures

→ 1st country to use blockchain at a national level for security purposes — Estonia
→ Instead of 7 months, blockchain helps to detect data misuse immediately
→ Estonian blockchain technology is available in more than 180 countries
→ NATO, US Department of Defence, European Union, Lockheed Martin, Ericsson etc. have all implemented Estonian blockchain technology
→ Every second, $10^{12}$ items of data are scaled by Estonian blockchain technology