UDC 338.2:004.9

M.Kovalchyk, graduate student
University of information technology and management in Rzeszow, Poland.

BLOCKCHAIN TECHNOLOGY IN GOVERNMENT DIGITALIZATION. ESTONIA CASE

The Blockchain is a chain of blocks that store the information – transaction records, not as traditionally, on centralized databases but decentralized among the participants of the network. Blocks are linked with each other by encryption and ordered chronologically. It ensures trust in the network. The decentralized way of transaction records storage allows participants of the network to keep up-to-date information. The mechanism of consensus in blockchain guarantees that the blocks of the network do not contradict each other. We can assume the blockchain network as a common ledger that is updated simultaneously in the whole network. The information stored in the network, once verified by the participants, cannot be changed or deleted - it can only operate in a way where a new record can be added. Therefore, it keeps all the transactions since the very first block was made.

The development of the blockchain technology is gone far away beyond the bitcoin – its first application. The management teams of a variety of companies from different fields are testing it and try to leverage a piece of the potential of this innovation. Transparency – one of the main benefits that technology can provide with.

Digital transformation is a trend that most of the governments want to apply. But digitalization has some threats and until today, the biggest problem and threat of such transformation was lack of secure way of operating with the data. It is understandable as any data misuse can lead to significant negative consequences.

The blockchain in Estonia.

Eventually, paper documents are no longer generated as everything is in the global trend of digitalization. The old files and documents are being archived or destroyed at all. Thus, the electronic ledger keeping all the data becomes very important for governments implementing digitalization process. All the efforts by the government towards the digitalization process to become the most electronic state required data security. Official authorities must protect the data from anything can violate it. In Estonia, this became especially clear during the so-called "cyberwar" in 2007, which was started, most likely, by the Russians and lasted for 3 weeks [1]. It was the first incidence of such an attack on the state by the state. Estonia, as a pioneer in the development of the e-government, was highly dependent on computers and the data in the network. Thus, the main targets of these cyber attacks were: the websites of the presidency and the parliament of the country; political parties, almost all of the websites of the state authorities; the biggest news agencies and other institutions [2]. After these cyber attacks, it was obvious that Estonia needed some security tools to prevent such threats in the future. Estonians understood that the risk of cyber attacks will always be as a part of digital society – a risk that must be prevented and taken seriously. In the country where the government transforms all the data to the digital one – a very safe approach is required. Therefore, the government started to look for a technological solution for such a relevant problem – protection of digital data.

Thus, the Estonian government started to test the Blockchain Technology as the tool to prevent the threats. As it is written in the official website of E-Estonia, the Estonian government has been testing the technology since 2008 – even before the white-paper of Bitcoin was published by so-called Satoshi Nakamoto, and it was called as "hash-linked-time-stamping". And since 2012, the technology has been already in use in Estonian e-state. It is being used in data registries like health, legislative, judicial, and other systems. It is constantly extending on other spheres as well. Therefore, we can say that Estonia is the leading player towards the blockchain revolution. Some misuses of the data are indeed hard to detect and it takes a long time to do so. Thus, in 2017 the study on the data breaches was conducted. According to the Ponemon Institute's and IBM research on a data breach, it takes more than 6 months to detect the data breach in the system [3]. In some cases, it takes even longer time to detect the breach. Thus, Yahoo was undergone by the data breach. It took more than 2 years for them to detect it and they still do not know exactly how it could happen [4]. The personal information of 3 millions of people was hacked and no one knows how it was used exactly by intruders. The blockchain technology can detect such breaches immediately. In Estonian blockchain network, we can see the data breach prevention as a high speed camera that is teleported within the network and detecting any misuse of the data. In the Blockchain network, such a machine is everywhere in the network and detects any violations. Moreover, it additionally detects how it was violated and by whom. The blockchain technology enables to detect any change of the original data, no matter how small it is, no matter by whom – immediately without any retards. It can be imagined in a way as "digital defence dust" that covers all the data. Thus, any change of the data will be detected through the prints left – like in the real-life crime. Blocks of the data covered by the "digital defence dust" are connected to each other in a chain that is distributed in nodes all over the world – like the nodes of the bitcoin network. Therefore, such distributed data becomes invulnerable for any data change so that no one knows it. In this way, the potential manipulation of the highly sensitive data, such as health records or any other personal information covered by the digital defence dust, is instantaneously detected. In the blockchain network used in Estonian government, a huge amount of data can be covered by digital defence dust as the blocks are connected to each other by a mathematically verifiable code and linked in a chain. Therefore, any data misuse cannot be done without leaving a trace.

The blockchain is a shared database meaning that data is not stored in a certain or single location. There is no centralized version of the data that can be hacked by any intruders. It makes the network safe to use. A blockchain vendor – Guardtime, a company behind the blockchain used in Estonia, have gone even further. Better safe than sorry, they publish the blockchain also on the physical media as well. Therefore, if someone wants to manipulate the data, then that intruder or the group of intruders will have to face not only the digital defence dust but also will have to replace thousands of physical copies all over the world. It is clear that no one can do so, therefore, we can assuredly say that the data on the blockchain is assumed as unchanging. As it was written above, while it takes more than 6 months to detect the data breach, the blockchain technology detects any breach or misuse of the data instantaneously. Thus, a case like Snowden in the National Security Agency of the USA would never happen if they used the blockchain technology as it would surely detect such a misuse of the data [5]. In order to make the data secure from intruders, instead of the original data, digital fingerprints called "hash values" are stored on the blockchain network. Thus, even if any intruders get there–there is no original data to be discredited. This technology resolves many problems which professionals were trying to resolve for many years. The blockchain does not only add more trust to the digital information but also function as a mechanism for verifying and correctness of the data. It is worth to note that nowadays, this technology developed by Estonians is also used in NATO and European Union to provide a cyber security.

In Estonia, since 2008, all the health records data of the citizens are available online. All the patients own their own data that is generated by the hospitals in digital format. The blockchain technology is used to provide the integrity of the health records and to provide the access to it. Almost all of the health information of the population is already integrated into the system. Medical receipts are issued online. It led to the uselessness of coming to the hospital in a variety of moments. An indeed convenient way for citizens who need to go to the hospital just to get the medical receipt. Transformation to the digital data is a win-win solution for both doctors and patients. Doctors are able to relieve the workload and patients are able to save the time for unnecessary visits. But health records data is a highly sensitive data that should be stored in a secure way and should be available only for authorized persons. Guardtime, an Estonian startup that develops the blockchain technology to secure private and public data, has signed an agreement with the Estonian government to ensure all the health records data of the citizens of Estonia with the blockchain technology. Guardtime developed a network that citizens, private companies, and state authorities are able to access the network to verify the data on it [6]. To do so, every citizen obtains a smartcard-ID that stores the citizen's personal data and provides an access to the great number of the online services provided by the state. Every access to the healthcare records is registered in the blockchain network. Neither doctors nor anyone else is able to change it. In most of the countries where the blockchain technology is not implemented you just have to trust to the medical institution. In blockchain, data being added to the network is verified by the majority of members of the network. Once it is signed-off - it cannot be changed. It uses a variety of copies so that even if one of it is compromised the data itself is untouched.

Exploring the case study on the real implementation of the blockchain technology in Estonia, it was realized that the blockchain can resolve such a problem as the data misuse. Estonia, as one of the most digital societies in the world as they provide almost all of the state services online, achieved the results where any data misuse can be detected and detected instantly. This result should not be underestimated as it provides an opportunity to provide electronic services that are beneficial for both the government and users - in a secure and transparent way. This successful implementation of the technology opens doors for every government that wants to deal with a digitalization process as the Estonians, as they say to the mass media, will be happy to share such an experience. To conclude, as this existing digitalization experience grows, this opens up opportunities for other countries such as Ukraine to seriously consider and to take advantage of this technological experience.

Literature

1. The Economist, War in the fifth domain. Are the mouse and keyboard new weapons of conflict? [at:] https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain, from 04.08.2018.
2. I. Traynor, Russia accused of unleashing cyberwar to disable Estonia, [at:] https://www.theguardian.com/world/2007/may/17/topstories3.russia, from 06.06.2018.
3. Ponemon Institute, Cost of Data Breach Study, [at:] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&, from 07.06.2018.
4. T. Hatmaker, Four years later, Yahoo still doesn’t know how 3 billions accounts were hacked, [at:] https://techcrunch.com/2017/11/08/yahoo-senate-commerce-hearing-russia-3-billion-hack/, from 23.05.2018.
5. K. Finley, How the Tech behind bitcoin could stop the next Snowden, [at:] https://www.wired.com/2015/06/tech-behind-bitcoin-stop-next-snowden/, from 03.05.2018.
6. O. Williams-Grut, Estonia is using technology behind bitcoin to secure 1 mln health records, [at:] https://www.businessinsider.de/guardtime-estonian-health-records-industrial-blockchain-bitcoin-2016-3?r=US&IR=T, from 05.05.2018.