Feasibility Study on the use of blockchain in public administration in the Republic of Serbia

Contents

Abstract

Ministry of Public Administration and Local Self-Government is publishing "Study on the Feasibility of Using Blockchain Technology in Public Administration of the Republic of Serbia", prepared by a team of young experts from Seoul, lecturers at Serbian-Korean Information Access Center, as part of the MPALSG project and the National Information Society Agency of the Government of the Republic of Korea.
It is a detailed analysis of the public administration system reform with the aim of sustainable development of Serbia through the application of new technologies. Blockchain security technology incorporates encryption techniques such as the creation of blocks and block hashes, which identifies blocks and merges them into chains, ensuring that personal information is permanently protected. This study provides a detailed elaboration of all the benefits of moving to this approach to the work of state authorities, analyzes the costs of introducing new technology in the most important areas and offers an assessment of the benefits and the level of savings that the Republic of Serbia can realize, and therefore its citizens.
With interest in and utilization of blockchain at home and abroad expanding, it is necessary to pay attention to the blockchain technology to solve problems related to the aforementioned reformation of Serbia's administrative system. Therefore, this report comprehensively analyzes the necessity of introducing blockchain technology to Serbia's public administration system, and examines the trend of blockchain introduction, focusing on discussions applicable to Serbia. Describe the principle of blockchain, and learn about the technology strategically through SWOT analysis. It compares the blockchain utilization cases in other countries and proposes how the government could apply blockchain to Serbian public services. It also describes the prerequisites Serbia must have for effective project progress.

Some problems with the introduction of blockchain have been pointed out, with a special emphasis on the fact that in one part of the public, primarily those residents of the Republic of Serbia who do not have adequate knowledge on modern technologies, there may be opposition due to the concern that personal data can be misused. Therefore, instructions have been given on how to introduce this technology so everyone can understand how it works and that it is completely safe and stable.
The study proposes that in order to improve e-government in Serbia, blockchain technology should be introduced into an integrated system of public administration consisting of land administration, agricultural product management and customs export system. Everything is graphically detailed as well, therefore it is easier to understand the whole process. Examples from several countries which are at different stages of the introduction of this technology are of great importance, as well as the analysis of everything that is included in their process of modernizing public administration. One of the conclusions that the Feasibility Study on the use of blockchain technology in the work of the public administration of the Republic of Serbia provides is that the use of blockchain prevents fraud and simplifies the transaction process.

1.What is blockchain?

1.1 Principle of operation

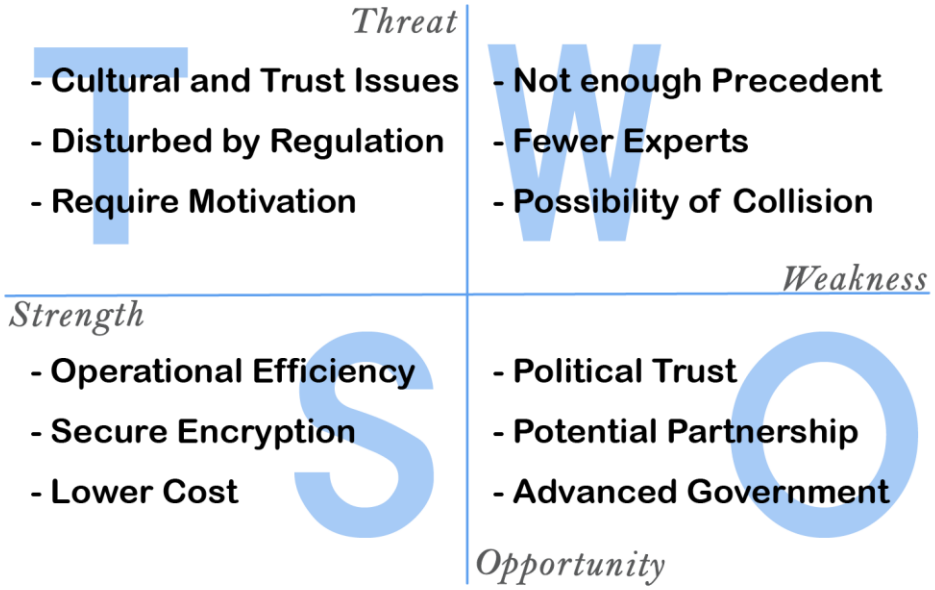
Blockchain is a security technology that makes the transaction safe by sharing and contrasting the entire transaction records of all traders. The blockchain contains the encryption techniques involved in creating the block and block hashes that identify and chain blocks. This ensures that your personal information and data are protected permanently.

A block contains a variety of information, such as a Merkle hash that contains transaction information and a block hash that identifies the block. Each block is created by mining, which has conceptually or logically linked chains because the newly generated block has a block hash that is influenced by the hash of the previous block. The blockchain also applied distributed ledger technology, so it can assure integrity.

The blockchain has solutions for vulnerabilities such as 51% attack and Byzantine Generals' problems and can choose various blockchain types and consensus algorithms depending on the situation. The consensus algorithm allows the blockchain to respond flexibly and immediately to malicious attacks. Also, various studies such as blockchain conferences are still strengthening the advantages of the blockchain and reducing the drawbacks.

By understanding and properly using the conceptual structure of the blockchain and the technologies applied, the Serbian government will be able to reduce the time and costs and provide convenience to the government and the public by using public services with blockchain.

1.2 SWOT(Strength, Weakness, Opportunity, Threat) Analysis



Strength

1) Operational Efficiency; sharing information with the electronic system can make government ministries become efficient in their operation.
2) Secure Encryption; Distributed ledger technology provides secure encryption and tamper-proof capabilities for critical data
3) Lower Cost; A distributed ledger of transactional data reduces storage cost compared to existing methods

Weakness

1) Not enough Precedent; As the few pilot projects and challenging uses, it is scarce to adopt the actual service.
2) Fewer Experts; Due to the immaturity and short history of the blockchain, there are a few experts and it is not a major agenda of the software companies.
3) Possibility of Collision; In the process of introducing a blockchain, there is a possibility of a collision that did not exist in the existing method. (Problems such as compatibility that have not occurred on traditional, well-distributed servers, one of the long-used and stable technologies, can occur by using blockchain.)

Opportunity

1) Political Trust; Transparency of blockchain voting enables to get the trust of the public.
2) Potential Partnership; Learning from the mature e-government opens the new and variable partnerships at blockchain project.

3) Advanced Government; Integrated large foundation data could advance future government plans.

Threat

1) Cultural and Trust Issues; Using blockchain on sensitive data can cause a social backlash.(It is difficult for lay users to understand blockchain easily. So it can't help to understand only the abstracted concept. When new technologies, such as block chains, are used on important issues such as government policy, it can weaken the reliability of technology and create a social backlash if users don't fully understand it's and security stability of the technology.)
2) Disturbed by Regulation; excessive regulation may restrict and obstruct the realization of value from the blockchain.
3) Require Motivation; To attempt the unfamiliar technology, it requires motivation for the software industry to get involved

2. Expected Utilization in RS

Serbia initiated an e-government project as part of the development of the information and communications sector by participating in the Electronic South Eastern Europe Initiative (eSEE). The Serbian government has enacted regulations and laws and continues to invest in ICT. Led by the prime minister of Serbia, the Serbian government is working on policy-making and concrete projects for the introduction of e-government.

In the UN's 2018 E-Government report, Serbia ranked 49th among 193 UN member states. The Serbian government currently operates an e-government portal (eUprava). This is quite high compared to most countries and offers a wide range of services. However, according to the Serbian Statistics Office, as of 2018, only 37.3% of Internet users use public services over the Internet, 20.2% of them use only for downloading information, and only 16.8% use public Internet services for submission of documents. To increase the low usage, the convenience of e-administration services should be enhanced to induce citizens' use.

In order to improve Serbian e-government, this study suggests the introduction of blockchain technology into the integrated administrative system, land administration, agricultural product management and export customs clearance system. Building an integrated administrative system using blockchain can increase the use of people by increasing the convenience of electronic administration, and the introduction of blockchain in land administration can increase the reliability of transactions and prevent the manipulation of transaction books. In addition, the distribution management and export customs clearance system using blockchain in the export of agricultural products, which is a major industry in Serbia, can enhance distribution transparency, enhance efficiency and simplify administrative tasks.

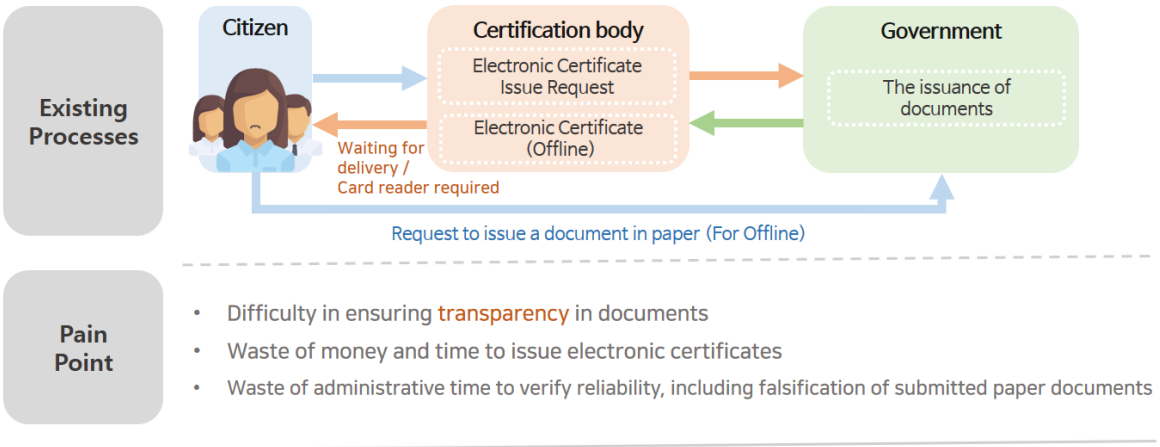
2.1 Integrated administration system

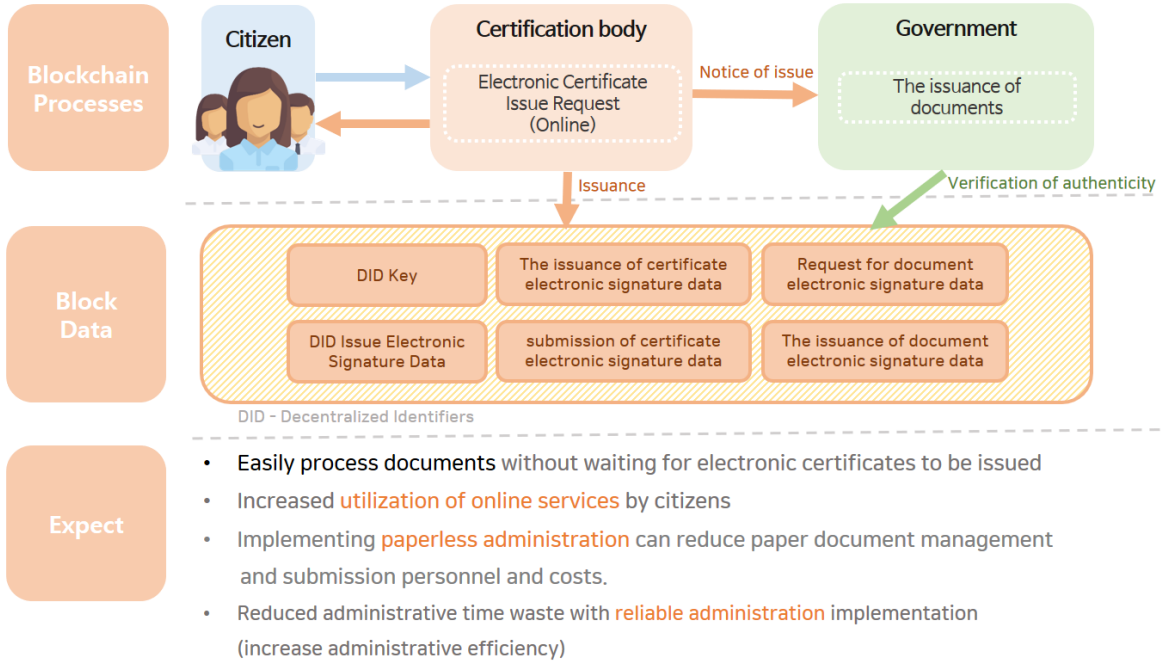
Serbia's e-government has reached the level where documents can be issued through electronic signatures on the Internet. This is the third phase of the UN e-Government development phase. Based on this, in the future, administrative automation should be achieved by establishing integrated administrative services among multi-ministries.

Existing e-government systems used by countries around the world are mostly centralized systems based on central servers. Representative challenges for centralized management systems are cost, time, and security. With centralized databases, central servers are primarily attacked. Most of the information is in the center. If the center collapses, all security will be compromised. Therefore, it costs a lot of security maintenance.

Distributed ledger technology, such as blockchain, is a way for each node in a distributed network to share and synchronize a database without the control of a central server. Because data is distributed and stored in many places, it can make up for the disadvantages of a centralized management system. In addition, all transactions that occur in the blockchain system are well documented and not easily manipulated, making them suitable for use in government systems that focus on reliability.

One of the biggest advantages of integrated administration using blockchain is simplicity. Unlike the existing system, the integrated administrative system using the blockchain shares information of all digital documents through the blockchain. The blockchain ensures the identity of the complainant, greatly reducing the complexity of the complainant's paperwork. Work between government agencies in charge of authentication and issuance can also be done more quickly using blockchain. Based on these advantages, a paperless administrative system can be built. This process can be expressed as shown below.





2.1.1 Case of another country

Estonia

Estonia is one of the countries with the most advanced e-government system in the world. Even before the blockchain emerged, Estonia had already built an integrated administrative system, and since 2012, it has been applying blockchain technology to X-Road, the national backbone network.

The original document is managed by the central server, but the hash value of the moment when the document is newly created is stored in the blockchain. If the original stored document is modified, the hash value is changed. Therefore, the hash value can be compared with the hash value stored in the blockchain to find out whether it is manipulated or not. There is little possibility that an electronic document can be manipulated. Therefore, if the electronic document and the paper document are different from each other and need to be authentic, the electronic document is given priority.

2.1.2 Estimated Costs

The estimated budget for integrated administrative services can be calculated as follows. This is the cost of replacing traditional servers with blockchain while maintaining existing integrated administrative services. Developers are needed to maintain existing integrated administration services (this is the cost of hiring existing developers and is not considered as an additional cost). Four blockchain developers will be needed(The unit price for each developer is $15,000 per month.). In addition, the costs required to maintain the service are not calculated as additional costs because only the cost of maintaining the existing service will be required. The expected final cost will be $ 360,000. The period requires six months.

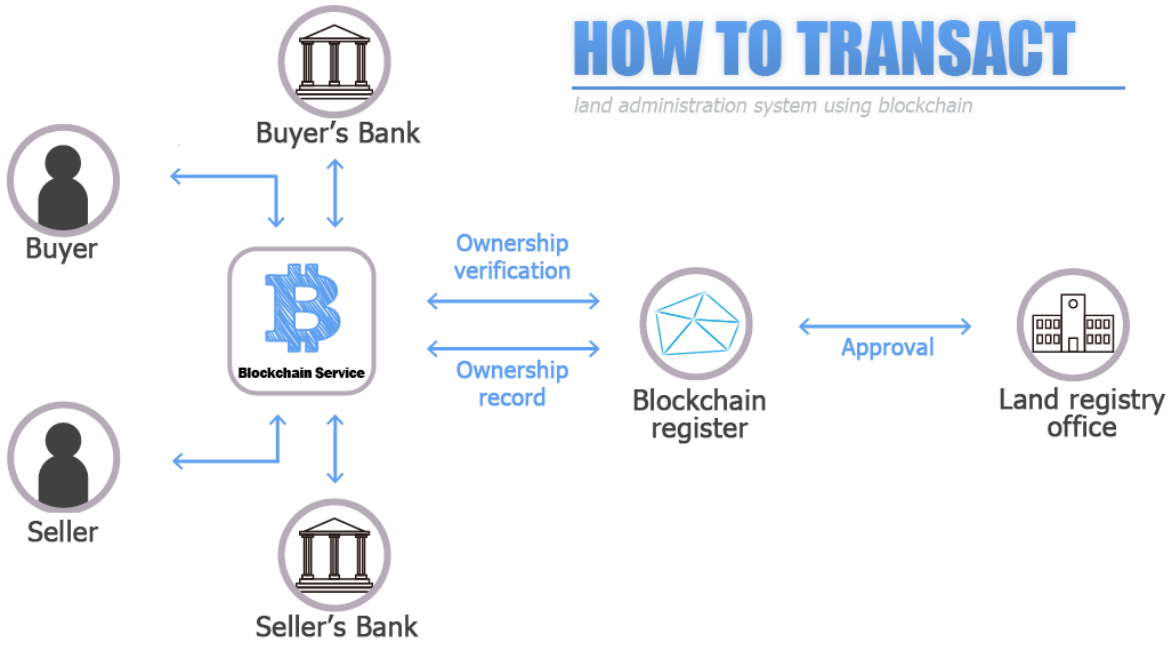
2.2 Land Administration

In 2012, around 10% business representatives considered that the payment of bribes to land registry officers in Serbia occurs very or fairly frequently in businesses like theirs .[1] Foreign investors have full private property ownership rights, yet, have insufficient confidence in the protection of these rights in practice. because enforcement of property rights through the judicial system can be very slow and a multitude of factors can complicate property titles – restitution claims, unlicensed and illegal construction, limitation of property rights to "rights of use," outright title fraud and other issues. Investors are cautioned to investigate thoroughly all property title issues on land intended for investment projects. [2] These problems reduce the efficiency of service delivery and undermines public trust in the government. The introduction of blockchain can prevent fraud and simplify the transaction process in land trading. Shared database with blockchain clarifies property ownership and provides latest ownership information. Institutions and government can clearly identify stakeholders when they purchase land or build new facilities. Promoting the free use of capital will improve economic conditions and create new opportunities for the poor, small businesses and SMEs.

[1] UNODC,"BUSINESS, "CORRUPTION AND CRIME IN SERBIA: The impact of bribery and other crime on private enterprise", (2013), p44

[2] US Department of State, "Serbia Country Commercial Guide",(2017), Investment Climate Statement, https://www.export.gov/article?id=Serbia-Executive-Summary WORLD ECONOMIC FORUM, "The Global Competitiveness Report 2017-2018", (2017)

A land administration system using blockchain can be expressed as shown below.



Seller registers the land to be sold. If there is a buyer who wants to buy the land and the deal goes on, All transaction details are recorded on the blockchain. At this time blockchain verifies the land ownership of the seller and approves the transaction. If there is nothing wrong, the transaction proceeds and new ownership is recorded on the blockchain.

2.2.1 Case of another country

Georgia

Georgia has developed a land trading platform with the goal of creating a healthy economic ecosystem by preventing tampering of ownership and contracts in real estate transactions. The whole process of land ownership registration, certification and sale can be verified by third parties and prevent manipulation. The system has already registered more than 100,000 land ledgers and is expanding the platform to add smart contract solutions.

Honduras

Honduras has been applying blockchain to the land contract system since 2015 to prevent civil servants from manipulating land registers. If the land ledger is managed by blockchain, it can prevent manipulation of the stored land details and transparently disclose the transaction details.

2.2.2 Estimated Costs

The estimated budget for land management services can be calculated as follows. Cost calculations are based on three situations: The costs of re-adjusting the applications used in existing land management services to change the structure to blockchain, the costs of constructing new land management services with blockchain, and the costs of organizing third-party applications that make new land management services available to relevant departments.

The functions required to implant data used in existing land management services are to be covered by four DB management experts (two in groups of one team, one team to collect existing DB data, and the other team to register data in blockchain). These developers will work on preserving the contents of the DB and transplanting existing data into blockchain. In addition, two blockchain experts will be needed for blockchain experts to record their contents in the blockchain.

The second is the cost of forming a new land management service into a blockchain. Four blockchain experts and four developers each needed to construct front-end and back-end applications.

Finally, developers who form third-party applications that make new land management services available to relevant departments need two front-end developers and two back-end developers. This can be done in the form of rebalancing programs for existing applications, but if there is a need to create new applications, two more developers will be needed each.

Although the cost for maintenance will depend on the amount of circular data in the service, typical commercial software, a global service, has assumed and calculated the maximum cost of this service, considering the need for maintenance costs of $ 10,000 to $ 100,000 per year using an external cloud server. The estimated period is six months and the expected final cost is $ 340,000.

2.3 Logistics and export

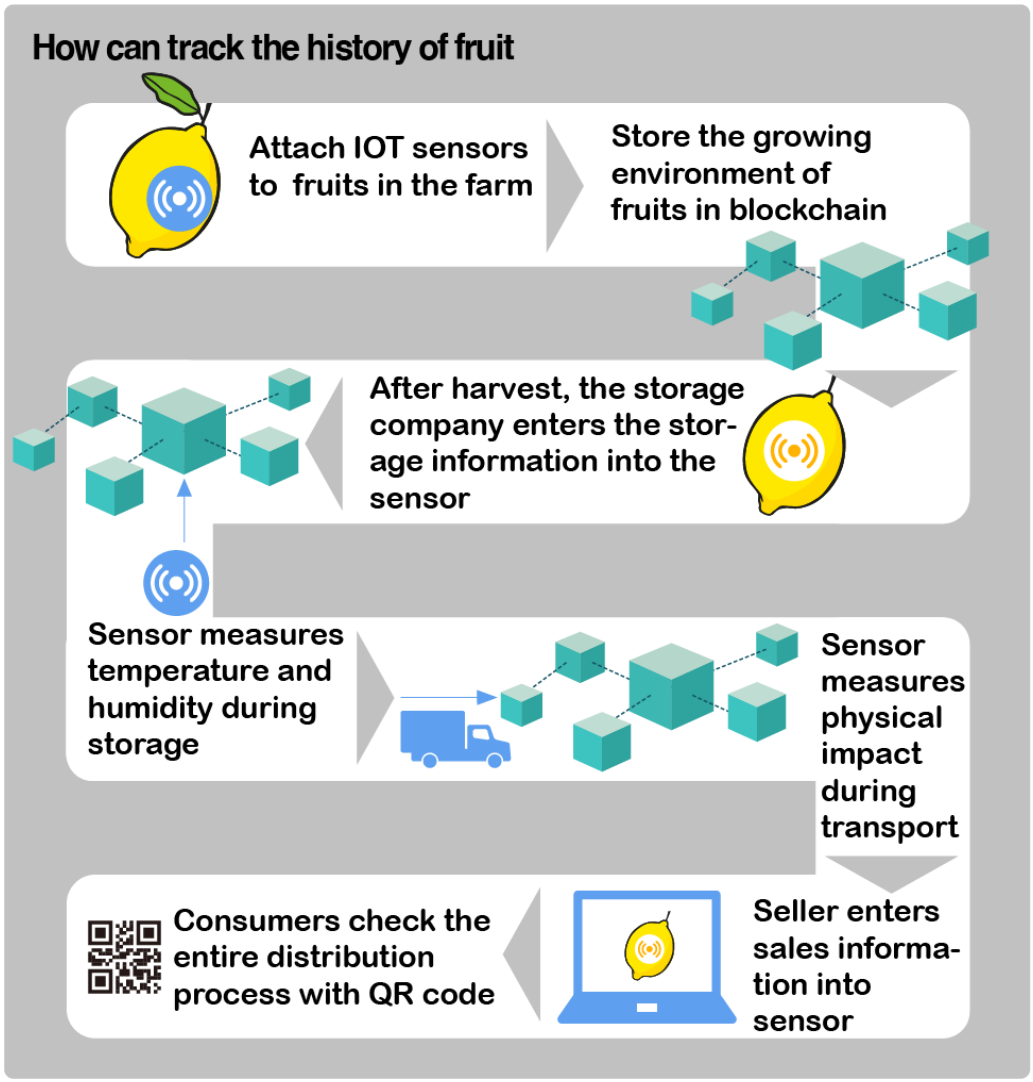
Agriculture in Serbia is at the heart of the economy and is an engine for development of rural areas. Agriculture's contribution to Serbia's GDP remains high. In 2016, agriculture accounted for 11.9 percent of GDP. According to the Serbian Statistical Office, there are 680,000 people employed in agriculture or 21 percent of the total labor force in the country. Agriculture is the most important export sector in Serbia. In 2016, agriculture and food production accounted for 19.4 percent of all Serbian exports.[3]

[3] The International Trade Administration, "Serbia Country Commercial Guide", 2018

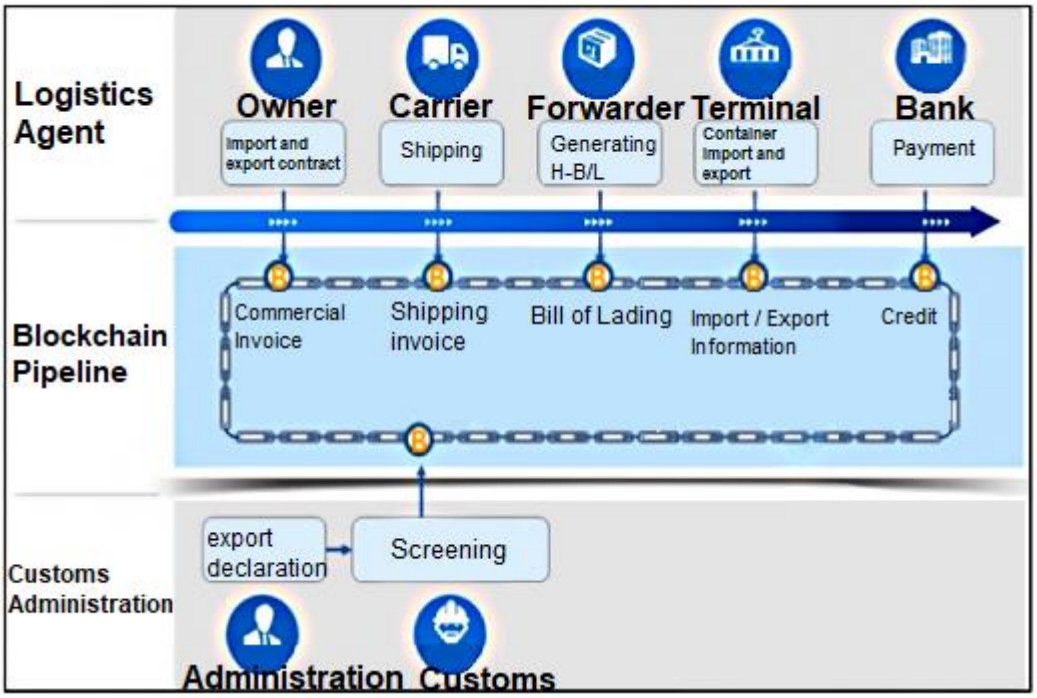
Blockchain can enhance the transparency of agricultural distribution systems. Using IoT sensors, all histories of production and cultivation of agricultural products are stored through blockchain service. When trading agricultural products, individual traders only keep their trade books up to date. Changes in the trading books are updated in real time through the blockchain, enabling instant tracking of trading information. All transaction history is transparent and can not be manipulated. Therefore, when a safety problem occurs, all transactions can be traced back to immediately grasp the situation and minimize the impact of the problem. All histories of agricultural products can be easily retrieved, increasing consumer confidence. In addition, the distribution cost is reduced by increasing the efficiency of the distribution process.

The export process of agricultural products involves a number of institutions and enterprises, including customs agencies, exporters, importers, banks, insurance companies, and terminal warehouses. Numerous documents are required from customs declaration of exports to final delivery. By using blockchain services in this process, all transaction information can be shared efficiently and transparently. All documents generated during the export process can be stored in real time on the computers of all institutions and enterprises through the blockchain to prevent document manipulation and to check the current customs procedures in real time, reducing administrative requirements and increasing efficiency.

A distribution system using blockchain can be expressed as shown below:



Export process using blockchain can be expressed as shown below.



2.3.1 Case of another country

Blockchain-based export customs clearance logistics service of the Republic of Korea

In May 2019, the Korea Customs Service launched a pilot operation of the world's first blockchain-based export customs clearance logistics service. Signed an agreement with 48 institutions and companies, including public institutions, shipping companies and insurance companies, to promote export customs clearance logistics services based on blockchain. All administrative procedures required for customs clearance are linked into one blockchain, bringing all procedures together. The Korea Customs Service aims to secure trade stability, real-time visibility, and streamline business procedures by increasing transparency and efficiency of trade procedures.

2.3.2 Estimated Costs

The estimated budget for export customs logistics services can be calculated as follows. In general, when a single developer is employed to create a typical blockchain application, it is expected to take $ 15,000 to develop the blockchain management system itself, given that the application front-end, back-end, design, and man-month is calculated. Assume that these 2 advanced developers are hired to develop for six months.(Given that the typical project is

divided into quarterly, semi-annual and yearly units, the average development period has been assumed.) In addition, the number of IoT-attached sensors that are needed per item.

In 2015, Serbia became the 1st in the world production of raspberries by country.
Taking the raspberry production market as an example, domestic raspberry production was 109,742 tons.[4]
Based on containers for export of 20 ft DV, loadable up to 18 tonnes. so All containers carrying raspberry require 6,096 IoT-attached sensors.

When using low-cost materials that take into account the necessary function, regardless of the material, consider the electronics that will be used to register information in the blockchain and use a $ 0.6 sensor per unit. This is because it depends on the function and sensor type required in the IoT.

The cost is $ 3,700. When an external cloud server paid for the equipment and equipment needed to maintain the service, it was expected to cost $ 100,000. Thus, the total estimate would be $ 473,700.

3. Prerequisites of utilization

Technology

Construction of quality telecommunications infrastructure is important to maintain a blockchain system. It should be expanded to prepare network traffic increase. Computerized data resources are needed to design the blockchain project. Therefore, existing data should be computerized. Moreover, in order to respond to data reliability, manipulation, and security problems, technical measures such as accurate authentication(biometric information such as fingerprints) are needed.

Resource

There should be blockchain experts for the maintenance and operation of blockchain systems and IT human resources. In addition, each government department should expand IT equipment and prepare work manuals so that the new e-government system can be used well. Above all, the project budget should be appropriated precisely so that the project can proceed smoothly.

System

To establish a benchmark for technology utilization, Establishing a definition of blockchain technology is a priority. It should be used as a measure of technology utilization based on the legal definition of blockchain. Based on this, the government will establish a link between industry and academia to promote the development of blockchain technology and establish measures to foster blockchain technology. In addition, the government should prepare

[4] Statistical Office of Serbia, 2017 Survey on Orchards: Results, (2017)

institutional arrangements and regulations for data manipulation and security issues to prevent malicious use.

Accessibility

When e-government systems that introduce new technologies are established, there will inevitably be gaps in information according to the level of information service by users. The digital divide increases entry barriers to new systems and reduces the effectiveness of introducing the system. To minimize this problem, the government should provide information service education to those with low levels of information services. It should also provide time for users to become familiar with new technologies, and use them in conjunction with existing technologies to reduce confusion.

Expected cost

The government's budget is limited, and it is tough to budget for multiple IT sectors. So global demand for blockchain developers is rapidly increasing, while supply cannot follow suit. Nevertheless, governments in some countries are actively pursuing blockchain projects.

For example, The South Korean government has agreed to invest $ 35 million in 2019's budget to develop blockchain technology and industry. Also, they selected 12 final projects for their development in the public sector. This year, the US Department of State has granted $ 800,000 for a pilot project that will develop a blockchain-based system to track the working conditions of factory workers at this years. Moreover, The Australian government has allocated AU $ 700,000($ 521,000) of the Digital Transformation Agency (DTA) budget to explore the use of blockchain for 'government payments'.

Since labor costs and productivity (on average, the number of programs that one developer can develop in one month) vary from country to country, the overall development scale should be determined first. As a result, development costs, additional labor costs, infrastructure, and SW costs should be determined proportionately. Next, the budget and expected time frame will be set in line with Serbia's domestic situation and infrastructure.

4. Conclusion

We recognize the technological potential of Blockchain as asserted in the introduction of this technology into the e-government system promoted by Serbia. First, by proposing measures for the establishment of paperless administrative systems and the shift to digital documents used in e-government deployment, we could foresee the benefits of seamless handling of civil petitions and increased administrative efficiency. We also advocate the introduction of a land management system that leverages blockchain technology to improve the land management system of Serbia, that currently lacks public trust. It is expected that Blockchain could not only

prevent fraud and simplify transactional processes in land transactions, but it could also improve economic conditions.

Lastly, in agriculture, which accounts for 11% of Serbia's GDP, we propose the introduction of Blockchain technology into the agricultural distribution system so that production and shipments can be managed more efficiently. The analysis suggests that all transaction information made during the logistics and export processes could be shared efficiently and transparently.

Further, the future ahead of us will be the age of data. The use of big data will become increasingly more important. Blockchain can enhance personal control of individual data as well as data security. Likewise, Blockchain will then be the foundation of all industries such as infrastructure. Currently, Serbia is not a country with an established e-government system, but it has set the stage for a flexible introduction of blockchain technology. In this regard, we are optimistic in leveraging the above three projects as a springboard for the establishment of e-government systems in Serbia.

5. References

UN, “UN E-Government Survey 2018”, (2018)

UNODC,”BUSINESS, “CORRUPTION AND CRIME IN SERBIA: The impact of bribery and other crime on private enterprise”, (2013)

UNDP SERBIA, “PUBLIC PERCEPTIONS OF CORRUPTION IN SERBIA Tenth Research Cycle”, (2015)

WORLD ECONOMIC FORUM, “The Global Competitiveness Report 2017-2018”, (2017)

The International Trade Administration, ”Serbia Country Commercial Guide”, (2018)

Statistical Office of Serbia, 2017 Survey on Orchards: Results, (2017)

Medium, Nov 12 2018, https://medium.com/linum-labs/swiss-federal-railway-trials-first-digital-identity-pilot-on-ethereum-4a3cb3c6621

SWISSCOM, Dec 06 2018, https://www.swisscom.ch/content/dam/swisscom/en/about/media/press-release/2018/20181206-mm-sc-post-privateblockchain-en.pdf.res/20181206-mm-sc-post-privateblockchain-en.pdf

Federal Office for Migration and Refugees, “Unterstützung der Kommunikation und Zusammenarbeit im Asylprozess mit Hilfe von Blockchain”, (2018)

Colm Hebblethwaite, GovCoin aims to disrupt UK welfare system, Blockchain Technology News, Nov 28 2017, https://www.blockchaintechnology-news.com/2017/11/28/govcoin-aims-disrupt-uk-welfare-system/

West Virginia Secretary of State, Feb 14 2019, https://sos.wv.gov/news/Pages/02-14-2019-A.aspx, https://sos.wv.gov/FormSearch/Elections/Informational/West-Virginia-Mobile-Voting-White-Paper-NASS-Submission.pdf

PATMENTS CANADA, "Jasper report", (2017)

Ministry of Science and ICT, Dec 18 2018, https://www.msit.go.kr/SYNAP/skin/doc.html?fn=b28cc1da2fb2791aabde52dae1702af8&rs=/SYNAP/sn3hcv/result/201907/

Government of Dubai, https://www.dubailand.gov.ae/English/Pages/ApplicationDetails.aspx?AppID=19

Event Horizon Summit, "Energy blockchain startups WHO-IS-WHO", (2019)

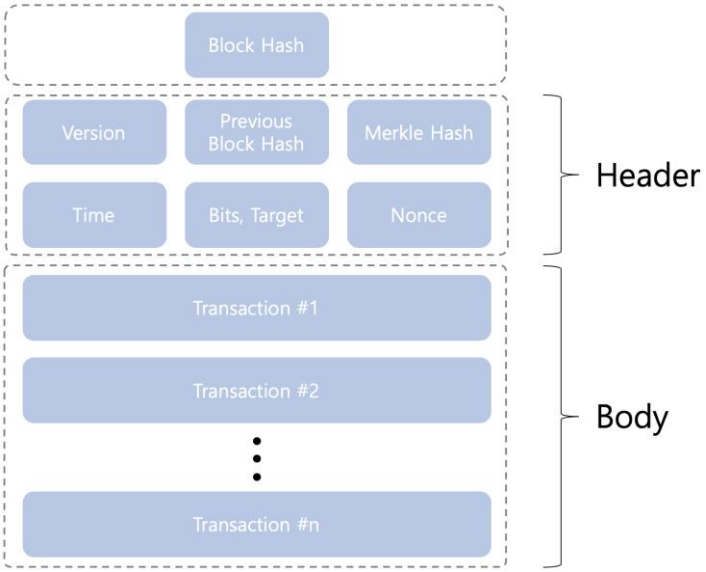
Korea Insurance Research Institute, Leverage Blockchain in the Insurance Industry, (2018)

6. Appendix

6.1 Technical description of blockchain

Nodes represent all traders. Each node can contribute to the network by participating in the behavior of the blockchain and ensuring reliability.

Every trader keeps a record of the transaction ledger in the blockchain and keeps them from counterfeiting and tampering by collating the information against each other.

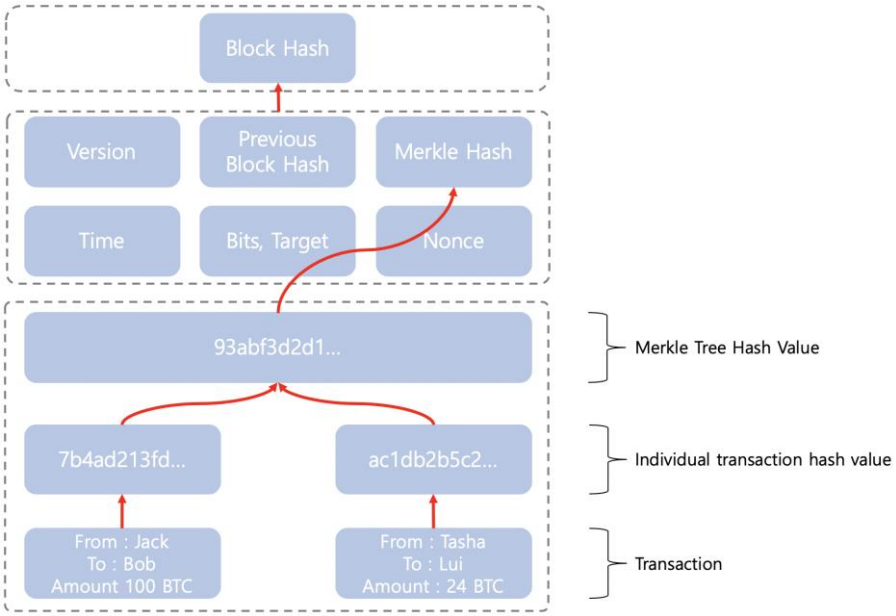


Each block in a blockchain is an element of a Blockchain. It is also called Height because it recognizes the block as a stacked form. However, the exact name of the block is Transaction ID (TXID), a Block Hash value. This TXID is the sum of all the information in the block and then encrypted. A block mainly consists of a Header and a Body. In Header, the information of the block and the block hash information, which is the ID of the previous block, are recorded. The body contains a bunch of transaction information and other information.

The encryption technology applied to the blockchain is SHA256. It compresses the information and displays it in a string of 64 characters so that it can store data efficiently even if the connection to the block in the chain is still. It is the recommended secure encryption technique for storing sensitive data in modern computer science.

The block hash serves as an identifier for the block. The block hash is the final value that is converted to SHA256 twice after adding the version (software or protocol) of the block's header information, the previous block hash (the block hash of the immediately preceding block in the Blockchain), Merkle root (the time at which the block was created), time (the time at which the block was created), bits (a value to adjust the degree of difficulty), Nonce (Number of calculation starting from the first zero and increasing by 1 until finding a hash value

satisfying the condition). Merkle root is a hash tree of transaction information stored in the Merkle hash, the body part of the block. The hash value is obtained by pairing each transaction and the nearest node, and the final hash value becomes Merkle root value. The Merkle hash value can be used to verify the integrity of transactions in a single block. Since the hash value of the block is generated using the Merkle hash value, the integrity of the block hash can be verified as well.



Merkle hash exists to ensure blockchain integrity. The hash value of the transaction information is used as a value in the Merkle hash calculation of the block containing the transaction and the Merkle hash is used as the input value of block hash calculation. Block hash is saved as the previous block hash information of the next block, and it is used as the input value to calculate the block hash of the next block. Therefore, if the transaction information changes, the Merkle hash changes, and so all values of block hash in the chain.
To change the completed transaction, all blocks after the block containing the transaction information must be re-mined in order, and it takes too much time, while other nodes continuously add blocks, hence changing information is practically impossible in practice.

Mining is a process of generating a hash block result by substituting an arbitrary Nonce value and connect to the chain by the work proof method which is one of the consensus algorithm. If we want to add a new block to a blockchain, the block hash of the new block must be computed by computing the nonce value, which is one of the block header information. The goal is to make the block hash value less than a certain number, calculated as one of the input values of this nonce value. If the repeatedly calculated block hash value increases by 1 and is less than the specified number, then the calculated block hash is confirmed, and the block with the identifier obtained is added to the blockchain as the new block and the operation is completed.

Distributed ledger technology refers to a technique in which participants jointly record and manage the ledger of transaction information on a distributed network rather than on a

centralized server in a specific agency. Distributed ledger technology has advantages in terms of efficiency, security, system reliability, and transparency compared to centralized methods. While existing systems require multiple intermediaries or certification bodies to authenticate and verify data transactions, distributed ledger technology has a distinction that allows users to share transactions directly. It is low cost because we do not have to maintain and manage central servers and centralized systems, and because transaction information stored distributed, there is minimal risk of hacking and forgery. On a distributed ledger-based platform, all processes such as verifying, disseminating, and recording transaction information are automatically implemented. As a result, transaction efficiency and processing speed could be increased.

A 51% attack is a potential threat to a public blockchain that allows a single entity or organization to control the blockchain, allowing them to disrupt the network. Attackers must own at least half of the stakes to modify or exclude blockchain intentionally. While the malicious user is in control, they can revert the transaction that someone attempted or caused, and it can lead to double-spending problems. If exploitation successes by attackers, they can prevent some or all of the transactions from being approved, prevent mining and monopolize mining rights.

In the Byzantine Generals' problem, a number of generals of the Byzantine Empire are to attack one enemy and to win the battle against the enemy, more than half of the generals must attack at the same time. However, generals can communicate only through liaison, and there is more than one traitor among generals, so how to agree on the attack timing becomes the most crucial matter.

There are three types of blockchain: public blockchain, consortium blockchain, and private blockchain. A public blockchain is an open and operational account for everyone over the Internet. Also, it can access anyone who provides computing power to the network. It is hard to scale and has low speed. A consortium blockchain is a semi-central blockchain. Only pre-selected users can participate through agreed rules between the users, and It is characterized by easy network expansion and fast speed. A private blockchain is a blockchain that allows only authorized persons to participate in the network. Participants are pre-qualified to participate in the reading, writing, and agreement processes. It can add or remove users as needed, making it suitable for use by government agencies.

A consensus algorithm is a kind of process used in computer science and is a concept designed to maintain the same value for specific data between decentralized systems. A Blockchain refers to a 'distributed ledger system' where many nodes are connected to a P2P network to process and record transactions. You must share the same transaction record with all Distributed Ledgers in the system. It is the consensus algorithm that allows a block to be created and linked by a specific mechanism so that all nodes can have the same chain. In other words, in a network with a time difference in information reach, such as a peer-to-peer network, a participant can get a consensus on a single result.

For an example of A's transaction record, there will be any confusion if there is a balance of 1,000 Dinars checked in Korea, but 5,000 Denars in Serbia. Thus the blockchain ensures to maintain the same data value by consensus algorithm; hence, the balances are in equal value,

whether in Korea or Serbia. If the consensus algorithm does not work correctly, such as data values manipulated by a particular node or double payments, the blockchain system loses its credibility, so the implementation of a valid consensus algorithm is the most critical issue. Double payment is a payment made several times with a single bill. For example, there are 1,000 Dinars in the account of A currently, and A is going to transfer 1000 Dinars to B and C respectively. In the real world, this is impossible. Because the banking system tracks and manages the A's account, it is blocked immediately. However, double payment on an online network is not difficult. It is not possible within the same device, but it is possible to connect and send from two physically distant points simultaneously. It means that A can send B 1,000 dinars to B and in Korea, and another 1,000 dinars to C in Serbia with the same wallet. In a Blockchain network, however, double payments are denied by the consensus algorithm. Because even if a double payment is made, all nodes share the same distributed ledger, so one day there will be a collision at a certain point, and one of the two transactions will be rejected as a result.

6.2 Use cases of blockchain technology

6.2.1 Use cases of technology by government

6.2.1.1 Use cases in Europe

1) Use case of The Swiss Federal Railway

The Swiss Federal Railway (Schweizerische Bundesbahnen, SBB) is a public enterprise in Switzerland with 3,200 km of railway tracks and about 32,000 employees to maintain and manage the railway lines throughout Switzerland. Of course, managing the track can not be absolutely free from the risk of train accidents, the Swiss government needed to keep records of who worked on the construction site and whether the person was certified. Due to the compatibility of blockchain technology in these credential management systems, SBB conducted a pilot project in Zug City for six months from May to November 2018. During the test period, workers were required to check-in / out at the construction site through the digital ID of the mobile application "uPort" (ether-based identification and user-centered data platform). As a result, the project proved the security level provided by the blockchain technology is improved in that a particular company does not own personal information alone.

2) Swiss Infrastructure

On December 6, 2018, the Swiss postal agency “SwissPost” and the state-owned telecom “Swisscom” announced a joint statement. They co-developed a private blockchain to build a simple, secure, and sustainable infrastructure. The blockchain, based on the Hyperledger Fabric 2.0 software, specifically for user-to-user identification as compared to public blockchains, is only available in Switzerland. Therefore it can greatly reduce the energy by quick and efficient work. In particular, this blockchain will be launched in the second quarter of 2019 and will be available to other companies, as a part of a national strategy that the Swiss government is investing in to occupy a leading position in the blockchain industry. Once the blockchain has

been successfully deployed, government agencies and companies that use it will be able to simplify collaboration and management tasks by sharing data in real-time for all users while maintaining confidentiality.

3) Use case of blockchain in immigration in Germany

The German Federal Immigration and Refugee Office (BAFM) conducted a blockchain experiment with the Fraunhofer Institute for Applied Information Technology (FIT) for four months from February to June 2018. One purpose of this experiment is to judge whether digital authentication of immigration is possible by using blockchain. The other is to create an improved information flow to support all government agencies involved in immigration. As a result, BAFM conclude that blockchain technology could improve the problem of asylum procedures. By providing biometric information mandatorily when an immigrant enters the country, the digital certificate of the immigrant can be perfectly documented without going through the paper process. As the data from asylum seekers shared and updated by all government agencies, it enables fast, efficient, and secure data processing. BAFM's report suggests that such a system should be adopted across the whole EU and it says "If we could build a blockchain-based personal authentication platform across Europe, personal digital authentication would help achieve European unification at a fundamental level."

4) Use cases in UK

-Preventing fraud and abuse by blockchain

In 2016, the UK announced the national blockchain technology adoption. The experiment of "Department for Work & Pensions (DWP)" is also an extension of the blockchain technology. The DWP employs about 11.6 billion euros a year for welfare benefits, but about 350 million euros are budgeted for frauds, miscalculations, and system errors. While trying to find a way to prevent waste, the UK government focused on blockchain technology and conducted experiments with 'GovCoin'. Twenty-four subjects received and paid wages using the mobile app during the trial period, and the transactions were recorded in the Distributed ledger. Using this stored information, DWP was able to filter out fraudulent recipients who spent money on inappropriate places and was able to easily catch and correct minor mistakes in the application or payment process. In addition, by using the blockchain, the welfare allowance is paid to the final beneficiary so that the benefits can be received directly, which can save money by streamlining the transaction procedure and reducing the brokerage fee.

6.2.1.2 Use cases in North America

1) Electronic voting in the United States

Starting with the 2016 electronic voting for the Texas Libertarian Party and the Utah Republican presidential nomination, at the time of the November 2018 general election, West Virginia was the first U.S. state to conduct electronic voting that introduced blockchain technology in 55 county constituencies.

This was done through a mobile application provided by Voatz, a blockchain solutions company, and the certification in voting applications is done by a three-step process utilizing the camera and biometric functions (with fingerprint or face recognition) of the smartphone. First, the voters must scan the photos of their driver's licenses. Then, they follow along with an in-app instructional video to shoot and send a video of their faces. Facial recognition technologies, like Apple's Face ID, are used to verify that the face in the video is the same, and the account is registered in the state's voter registration base.

After the account is registered, users can submit their votes through the app so long as their identities are verified with Face ID or by their fingerprints.

Voatz announced that they have successfully test-run through several cases more than 30 times, including state conventions to student council elections. In West Virginia, 13 absentee ballots were put in place in May last year in two county constituencies, and the pilot made it easier for a total of 144 soldiers in 30 countries to attend absentee ballots in last November's general elections.

West Virginia's Secretary of State Mac Warner said "For the first time in U.S. history, soldiers and expatriate were able to vote in federal elections using mobile devices. Without this technology, many of these soldiers and people would not have had the opportunity to participate in democracy."

"The biometric information device of the application, combined with blockchain technology and the proven digital path of voting paper, will be a safe alternative to the cumbersome absentee voting process that has traditionally been used," he said.

The State government of West Virginia, which has tested the possibility of electronic voting using blockchain technology, plans to expand it to the state in next year's presidential election, according to a report.

Denver, Colorado, is also trying to increase transparency and convenience in elections by introducing blockchain technology across the U.S., including conducting electronic voting in collaboration with Voatz from March 23 to May 7 this year.

2) Interbank payment of Jasper Project in Canada

'Jasper Project' held by the Canadian government is the first blockchain experiment in the world in which the central bank has partnered with a private financial institution, and was launched in early 2016 with the aim of stabilizing the interbank payment method using DLT, and focusing on the operation of technology, legal, policy, and related regulations.

Media reported on May 2 (local time) that Bank of Canada and Monetary Authority of Singapore (MAS) have successfully tested cross-country payments using blockchain technology and Central Bank Digital Currency (CBDC).

Monetary Authority of Singapore evaluated through a statement that the test has shown the potential to increase the efficiency of cross-border payments and to reduce the risk burden.

The test involves connecting the blockchain platform 'Ubin' of Monetary Authority of Singapore and 'Jasper' of Bank of Canada, which are equivalent to the DLT network of the two banks and transferring funds from the BAS to the BoC without going through a third agency.

In this regard, a market research firm, Juniper Research, has proposed that banks can save about 11% of their operating costs using blockchain when addressing the financial business segments.

6.2.1.3 Use cases in Asia-Pacific

1) Use cases in Korea

- Innovation of port logistics by blockchain

On December 18, 2018, the Korea "Ministry of Science and ICT" and "Ministry of Oceans and Fisheries" announced the "Integrated issuance service for container import/export" based on a blockchain for port logistics innovation. This is one of the core tasks of 'BlockChain Technology Development Strategy' announced in June of the same year and will be operated for one year in Busan, the largest port in Korea. Busan Port has the second-largest transshipment volume in the world (No. 1 in Singapore), and ITT (International Terminal Transportation), which transports cargo to other ports, accounts for 16% of total transshipment volume so that sharing information between Shipping company and terminal operator is important However, this process was inefficient due to frequent modifications and delays caused by data omissions and communication errors, while communicating information using means of communication such as wireless/email/fax. To address this problem, if the information needed for transshipment is stored in the blockchain and shared in real-time, unnecessary work time generated by information inconsistencies between logistics entities will be reduced, and the convenience of transport operations will be increased.

2) Use cases in UAE

- The UAE is want to adopt AI and blockchain technologies in all economic, health, education and other important areas, and is promoting cooperation various government, federal and local agencies, international enterprises and venture businesses. They aim to transform 50 percent of government transactions into blockchain platforms by 2021 through Strategy for Artificial Intelligence. As part of this project, the Dubai Land Department introduced a blockchain-based Real Estate Self Transaction System in 2018 to simplify the process of intermediating between

lessors and tenants and digitizing paper documents. Also, on December 9, 2018, Abu Dhabi National Oil Company (ADNOC) announced a blockchain-based integrated oil and gas production management system in cooperation with IBM. This allows ADNOC's operators to automate the accounting process by exchanging real-time financial values from production to trading of crude oil.

6.2.2 Use cases of technology by private organizations

6.2.2.1 Use cases in Europe

1) Examples of Europe's power market

When blockchain technology is introduced into energy trading, it enables the free direct trading of P2P in real-time without the involvement of large utilities, significantly reducing the cost of interim transactions between power generation and consumers, leading to lower electricity prices.

In addition, all transactions are recorded on the network to ensure the security, transparency, and economics of the transaction, and to supplement power generation fluctuations due to weather conditions that are cited as weaknesses in renewable energy.

Germany's power market was completely liberalized in 1998, and there are now hundreds of utilities. Too many electricity companies and policies can also cause consumers to panic, such as a flurry of hype and the bankruptcy of an electricity company in use.

Not only Germany but also other countries in Europe are facing increased competition in the electricity market, and direct trading of P2P energy using blockchain technology was introduced in the UK on April 2018, which greatly reduced electricity prices and greatly reduced citizens' electricity bills.
With the new energy trading method, residents can buy and use the cheapest electricity in a time period without the need for power operator intervention, saving about half of their electricity bills.

The first technology to be introduced in the UK is the Hackney housing complex in northeastern London, which is divided into 13 blocks, and solar panels are installed on rooftops, measuring the demand and supply of energy for each household that monitors electricity generated from each block in real-time, so that it can be bought and sold automatically.

By using public electro power first and selling the remaining electricity to neighboring blocks, Verv Smart Hub, a renewable energy trading platform developed by AI(artificial intelligence), machine learning and startup Verv based on blockchain.

Not only Great Britain but also the United States, France, Australia, and many other countries are starting their blockchain energy industry.

In France, power grid operator Enedis, along with General Electric, introduced a blockchain-based energy trading system in the southern French city of Caro, which improved energy efficiency.

2) Other examples of insurance and financial industry

In other areas, German insurance giant Allianz SE applied blockchain technology to its insurance products, using smart contact for air delay insurance. If the flight is delayed until a certain time, the smart contact will be required to automatically arrive a notification message on the mobile phone and enter the bank account number to receive the insurance money immediately.

In addition, BNP Paribas, the largest bank in France that used bank letters of credit to purchase goods between companies, performed the work of converting all paper letters into safe distributed ledgers and applied blockchain technology to the financial industry, including completing the first blockchain-based letter of credit with HSBC Singapore in November 2018.

In other cases, Spain's second-largest bank, BBVA, issued its first blockchain-based cooperative loan in November 2018 to enhance transparency, stability, and efficiency of the loan process, lending to the utility.

6.2.2.2 Use cases in North America

1) Private Enterprise Medical Information in U.S

HealthVerity, a Philadelphia-based medical software provider in the United States, aims to eliminate the role of a third party by using blockchain to grant data owners access permission to information. It is particularly used in areas where such as cancer and rare diseases that the patients themselves must actively participate in their medical processes, and HealthVerity collects data and consents from patients, providing them to the medical institutions in need, thereby simplifying the interim process and enabling more efficient information transmission, while abiding by the Privacy Act. This also influenced to create a new model for monetizing patients' data in the healthcare industry.

In addition, blockchain technology is actively used in healthcare and medical industries as shown in Figure 2 below.

Blockchain	explanation
MedRec (U.S)	Built a blockchain platform to share information on patient care and it aims to implement interactive electronic health records.
Gem Health (Canada)	Formed a blockchain with the aim of establishing a shared identity system that can be utilized in various areas such as drug supply networks, automobile insurance, and social-based services.
Mediledger (U.S)	Developed a platform for drug transport and supply management, designed to enable interoperability of all prescription drugs to identify and track the supplied medicines.
BlockMedX (U.S)	The worlds' first solution for doctors to send prescription of certain drugs like an opioid, that are controlled by the U.S. Drug Enforcement Administration, to pharmacists.

6.2.2.3 Use cases in Asia-Pacific

1) Examples of Asian insurance industries
Blockchain technology is also one of the biggest concerns in the Korean insurance industry.
In 2018, Kyobo Life Insurance Co., a major life insurance company in Korea, introduced blockchain technology into the insurance payment system for the first time in Korea to automatically transmit mandatory records and claims from medical institutions to insurance companies through blockchain
authentication.

Based on the blockchain, personal identification is simplified so that the claim process can be carried out conveniently. The process of insurance claims is possible through the establishment of a common network, which requires certification to both the insurance company and the medical institution; thus, the management of insurance information and statistics is easy.

In September 2018, the People's Insurance Group of China announced that it would introduce blockchain technology to reduce insurance processing time and prevent fraud.
After installing blockchain platforms, it will apply insurance products based on IoT-based devices to provide quick compensation.

2) Examples of Asian financial industries
KB Kookmin Card in Korea was the first financial company in Korea to introduce a personal authentication system using blockchain technology to replace the existing Korea authentication system.

Furthermore, the bank succeeded in transferring the money from KB Kookmin Bank's Korea headquarters to the Tokyo branch using distributed ledger technology, and Korea's banking

sector launched a blockchain-based certification system in August 2018 to replace the existing public certificate.

In addition, when collecting and clearing checks, other bank's checks require at least one day, but blockchain can reduce processing time.
Tokyo-Missbish Bank (BTMU) of Japan has conducted a proof of concept (POC) and is working on it in conjunction with Hitachi Asia of Singapore.

3) Asia's production industry example

The information about fake foods in China can be easily heard from the news.
Disbelief and fear in food products ranging from fake eggs to rice, tapioca, and seaweed are prevalent.

In response, Wal-Mart in China has introduced IBM's blockchain-based food tracking platform, Food Trust, to ensure the entire cycle from production to distribution to trading, thus increasing food reliability. For each step of the supplier's delivery of food to consumers, detailed information of the food is recorded in the blockchain in real-time to enhance reliability by making the distribution process transparent.

The first case was done with pork selection. First, we attach an IoT sensor to the pig to store the breeding environment and breeding method in the blockchain. Second, the processing company enters the processing information into the blockchain to store the slaughtering process in the blockchain. Thirdly, the attached sensor records the transportation environment in the blockchain, and finally, the wholesale and retail company enters the information related to the sales environment in the package sensor to ensure the reliability of all information from production to consumption.

In addition, on June 3, 2019, Wal-Mart joined the Medie Leisure Consortium and made efforts to track and verify medicines using blockchain technology, not only for food, but also for the distribution of medicines, to improve the work of dumping medicines, fraud, and late payment due to the delayed payment.

6.2.3 Use cases of technology by international organizations

6.2.3.1 UNWFP (Ethereum based Remittance system for refugee)

UNWFP is one of the largest humanitarian organizations in terms of budget. They are working in over 80 countries and providing assistance to people in the food crisis. There are several ways of assistance. Among them, direct cash transfers can be the most efficient way for people in need. It is most effective and can also improve local economies. UNWFP provided cash transfers of $ 1.6 billion in 2018.

Traditionally, providing cash transfers to beneficiaries depends on multiple banks and other financial intermediaries. This increases remittance cost, introduces delays, and raises risks

around financial mismanagement and the security of beneficiary data. These issues are worse in regions dominated by hostile regimes, or high levels of corruption.

UNWFP initiates 'Building Blocks' project which facilitates cash transfers while protecting beneficiary data, controlling financial risks, and making remittance cheap. Using blockchain, a type of distributed ledger technology, the costs issued by third-party institutions can be eliminated up to 98% and the beneficiaries can receive remittances even in the event of an emergency situation.

This system of UNWFP relies on biometric registration data from the United Nations High Commissioner for Refugees(UNHCR). Refugees use their biometric data for authentication purposes. They can purchase food from local supermarkets in the camp by using the scan of their iris instead of cash, vouchers, or e-cards.

UNWFP did an initial pilot in Pakistan in January 2017. This project, which was aimed at 10,500 people used public Ethereum blockchain. After that, a more extensive pilot in the Azraq refugee camp in Jordan was initiated. This was aimed at initially 100,000 up to 500,000 people. In these camps, people are using blockchain-based computing platform by means of entitlements.

The beneficiaries could go to an authorized local store to purchase goods they needed. Food vouchers which have been used for many years have gone. Now, over 100,000 people living in the camps can purchase groceries by scanning an iris at checkout. Upon scanning the beneficiaries' irises, the blockchain backend authenticates the individual's identity via a linked relational database with hashed information on beneficiaries and their entitlements. Transactions are then recorded on the blockchain, creating a record of refugee expenditures. Vendors use a blockchain wallet to track transactions and receive payment for their sales directly from UNWFP.

In the 'Building Blocks, blockchain technology complements the existing digital platform and approach. The way beneficiaries use the cash remains the same, but backend data processing becomes more efficient as beneficiaries' identities can be confirmed, and cash distributed, without reliance on costly verification processes performed by banks and other institutions.

'Building Blocks' relies on a three-pronged technical approach comprising blockchain, digital database, and biometrics. This integrated approach is a challenge from a technical point of view and also the reason for the project's initial success. Recently, it has been funded €2m by Belgium. It is expanding not only in UNWFP activities in other refugee camps in Jordan but also in collaboration with UN WOMEN widely.

6.2.3.2 UNDP in RS (Blockchain-based diaspora remittances in RS)

UNDP is the largest multilateral technical assistance organization in the world based on the spirit of the UN Charter

In November 2016, UNDP Serbia was invited by the city of Nis to take part in the "Forum of Advanced Technologies in the City of Nis". On that occasion, discussions were held with diaspora individuals and representatives of private-sector companies whose employees receive remittances from abroad. Forum participants shared their opinions that remittance systems which are more transparent, faster and less expensive than traditional bank or financial services companies are needed.

Diasporas send money to ensure the wellbeing of their families back home. Their income contributes to the national economy greatly. Almost 800,000 people receive money from abroad. The estimated value of remittances, sent every year via official and unofficial channels, is approximately €4.5 billion. Annually, remittances make up close to 9% of the GDP, compared, for example, to direct foreign investments, which were 5.4% of annual GDP in 2016.

Reflecting these issues and needs of local actors, UNDP designed "Blockchain-based diaspora remittances in the city of Nis" project, to test how this kind of new technology can be of use to the government while making the financial transfer services cheaper, more transparent. Recently, the national bank of Serbia endorsed the pilot project conducted by UNDP, since the bank itself had already had a plan to test blockchain technology and to introduce potentially.

UNDP partnered with the AID:Tech Ltd., a private company from Ireland, well known and recognized for its innovative technological solutions for the humanitarian and development sector, and the U.S. company Stripe, specialized in safe online payments. Additionally, the national Komercijalna Bank is involved.

This project is open to all the citizens from abroad who send money to their families living in Nis. Senders from abroad simply log on to a platform donated by AID: Tech company, and send money in the amount $ 100 or € 100 using blockchain. Once the remittance is made, the recipients in Nis get the QR code on their mobile phone or email. By electronic readout of this code, the recipients can purchase goods at the stores in Nis, and pay the Public Utility bills.

It aims to contribute to reduce inequalities, and the achievement of the Sustainable Development Goal number 10.c, which states that by the year 2030, transaction costs of migrant remittances should be reduced to less than 3%, while remittance corridors with costs higher than 5% should be eliminated.