The Advantages and Disadvantages of the Blockchain Technology

Julija Golosova
Dept. of Modelling and Simulation
Riga Technical University
Riga, Latvia

Andrejs Romanovs
Dept. of Modelling and Simulation
Riga Technical University
Riga, Latvia

***Abstract* — The Blockchain is the newest and perspective technology in modern economy. This technology can help to solve different kind of problems in the industrial sphere, such as trust, transparency, security and reliability of data processing. In theory, the use of Blockchain technology shows great and positive results, but what can say about practice? In this paper the description of the Blockchain technology, and it advantages and disadvantages are analyzed. Many already implemented applications of Blockchain technology were studied, as well as affected success or problems factors during the implementations. This paper aim is to analyze conveniences and difficulties, related to the Blockchain integration and implementation in the different fields of modern industry.**

Keywords — *Blockchain technology, industrial cases, Blockchain implementation success factors*

I. Introduction

The Blockchain technology will promise us the bright future. It can help to make the business, government and logistic systems more reliable, trusty and safety. This technology has very strong benefits, because it can help to achieve the above goals in different systems. Certainly, the Blockchain technology has some disadvantages, mostly they relate to the costs and the implementation process of the technology. The successfully implementation of the technology is depending on many different factors, such as government and legislative support.

Certainly, the Blockchain is the new type of a database. This technology is very interesting for people, because it can solve one of the big problems, which are connecting with finance. This problem is a double spending without middleman. How does the Blockchain technology work and solve this problem? The Blockchain creates the blocks with different information. Each of these blocks relates to others blocks in this blockchain. The proof-of-work is used for the Blockchain's secure and safety. When the new block is connected to the Blockchain, it is almost impossible to change or delete these blocks. For the hacking of the Blockchain it is necessary to have very huge processing power. The miners are the people, who calculate the hash value for the new blocks [1], [3].

The Blockchain technology always relates to the cryptocurrency, because this technology is the basis of cryptocurrency's work, but these are different things. The Blockchain technology also is used in another areas, such as the logistics systems or medicine institutions and others. The application of this technology improves the quality of the system's working process.

In this paper is written about Blockchain technology benefits and challenges. The main advantages of the Blockchain technology are decentralized network, transparency, trusty chain, unalterable and indestructible technology. In turn, the main disadvantages of the Blockchain are the high energy dependence, the difficult process of integration and the implementation's high costs.

II. About Blockchain Technology

A. The definition of the Blockchain technology

"The blockchain is an incorruptible digital ledger of economic transaction that can be programmed to record no just financial transactions but virtually everything of value" – this statement is one of the most popular definition of the Blockchain, which is developed by Don and Alex Tapscott [1].

B. The structure of the Blockchain technology

The Blockchain consists of linear sequence blocks, which are added to chain with the regular intervals [1]. The information in the blocks depends on the Blockchain network, but the timestamp, transaction, and hash are existed in all the Blockchain variants.

Each block contains the cryptographic hash of the previous block (Fig. 1). All hash's information is generated automatically, it means that it is not possible to change any information in the hash. In this case, each next block amplifies the verification of the previous block and the secure of all Blockchain. The more blocks in the chain - the safer and more reliable the Blockchain [32].

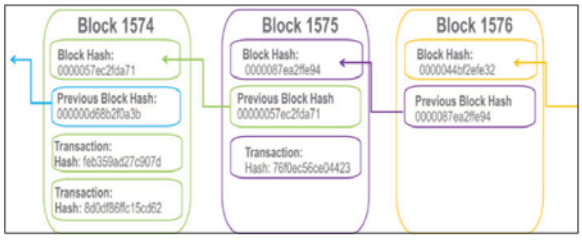

Fig. 1. The sequence of the hash value in the Blockchain [33].

978-1-7281-1999-1/18/$31.00 ©2018 IEEE

The Fig. 2 shows the signing process, which includes the signing with the private key and certificate. When the signing process has finished, then the verification process is started (Fig. 3). The verification is valid, if the hash values are the same.

Fig. 2. The signing process in the Blockchain.

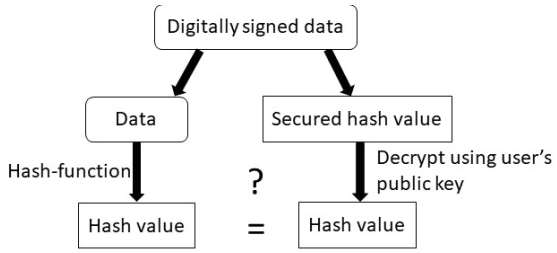

Fig. 3. The verification process in the Blockchain.

The Fig. 4 very simple shows, how blocks signing and verification processes work in the Blockchain.

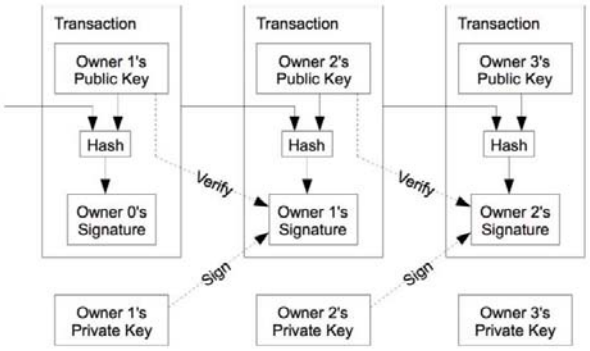

Fig. 4. The signing and verification processes [17].

Also, each block contains the "Timestamp", which shows the time of block creation. The transparency of the Blockchain is achieved by the registration of each transaction – it allows viewing the information of transaction at any time and it is public for all users of these chains. The transactions include the messages with the information to Externally Owned Accounts (EOAs) or contract accounts. The file JSON contains the public-private key and it is created when the new EOA is created. The private key of the sender is necessary for the sign the transactions. In turn, the private key and the account password are necessary for sending transactions to other accounts. The message is produced by the contract, but the transaction is produced by the EOA [1], [2], [32].

The time of the block generation is checked when the Blockchain receives the new block. The next block with all accumulated transactions is created through the 120 second after the time when the last block was signed by the miner on the 0 level.

The process of the block creation is shown at the Fig. 5. In this case, each block included the previous hash value, the timestamp, the merkle root and nonce.

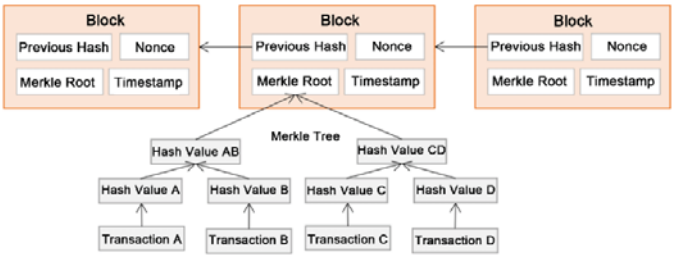

Fig. 5. The structure of the Blockchain [1].

C. *The properties of the Blockchain*

The Blockchain has different parameters, which are calculated, if the following properties are known [5]:

- headersize;
- transaction size;
- nodes in the system;
- mining power per node;
- bandwidth (b(i,j));
- blocksize;
- difficulty cryptopuzzle.

The last two properties are chosen.

The calculated given parameters are showed in the TABLE I.

TABLE I. THE CALCULATED GIVEN PARAMETERS OF THE BLOCKCHAIN [5]

Parameter	Formula
Total mining power	= ∑ m(i), i ϵ nodes
Number of transactions per block	= (blocksize – headersize) / transaction size
Block frequency	= total mining power / difficulty cryptopuzzel
Inter nodes time	= blocksize / b(i,j)
Transactions / second	= (blockfrequency / 60) * transactions per block

D. *Access to the Blockchain data*

The Blockchain technology has four varieties, which are classified based on access to the Blockchain data [32]. The TABLE II. shows this classification and the definitions of the classes [20].

TABLE II. THE FIRST CLASSIFICATION OF THE BLOCKCHAIN [20]

Name of the class	Definition
A public Blockchain	Does not have any restrictions on reading of the blocks and on submitting of the transactions for inclusion into the Blockchain
A private Blockchain	Has limited to a predefined list of users of the direct access to the blocks and submitting transactions
A permissionless Blockchain	Does not have any restrictions for the users which are eligible to create the blocks of transactions
A permissioned Blockchain	Has the list of the predefined users which are eligible to performed to process the transactions

Another classification is based on the processing of the transactions and the access of the data. The Blockchain can be not only private. The TABLE III. shows that the Blockchain has multiple levels of access with different opportunities [20], [29].

TABLE III. THE SECOND CLASSIFICATION OF THE BLOCKCHAIN [20]

Access to the data	The processing of the transactions	
	Permissioned	**Permissionless**
Public	Proprietary colored coins protocols	Existing cryptocurrencies (Bitcoins)
Regulated	The direct access to the reading and creating of the transactions for clients and regulators (limited)	Colored coins protocols (Colored Coins Protocol) which can limit to creating of the transactions
Private	The direct access to the data of the Blockchain is limited and the advantages of the Blockchain are partially lost	It is not possible to apply

E. Proof of Work (PoW)

The Proof of Work is the algorithm of the security. The mining is the process of solving a computational challenge imposed by the PoW protocol. The node, which wants to participate in mining, uses the PoW protocol for the affixation the block to the Blockchain. In this case, the node must choose the block with biggest hash's value and after that it can attach the block [7], [22], [23], [26], [31].

F. Proof of Stake (PoS)

The minting is the process of solving a computational challenge imposed by the Proof of Stake protocol. This protocol requires far fewer the computations for the mining. The trusted entities work together to add records in PoS protocol and there is the voting process for accepting the block on the Blockchain [7], [22], [23].

G. Smart Contracts

The smart contract is the script which is stored in the Blockchain. The smart contract has the unique address, set of executable functions and state variables. The user launches the smart contract by addressing the transaction to it. After that, the smart contract is automatically and independently performed in the established order on each node of the chain, depending on the data, which contained in the running transaction [1], [2], [22], [34]. The Fig. 6 shows the structure of the smart contract.

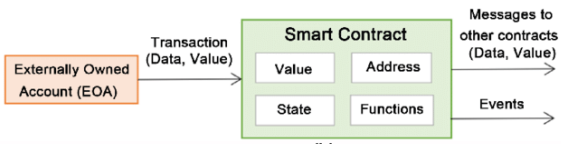

Fig. 6. The structure of the *smart contract* [2].

H. Ethereum

The Ethereum is flexible the Blockchain platform which is open to using by everyone. This platform has the high level of the security from different kind of the attacks. The users can create the Smart contracts and the decentralized applications. This platform is based on the Ethereum Virtual Machine (EVM) [2], [14], [18], [34].

The Ethereum platform has four processes [19]:

- block validation;
- network discovery;
- transaction creation;
- mining.

III. THE BLOCKCHAIN TECHNOLOGY CASES

The Blockchain technology can be used in the different industrial and technical areas. The biggest IT companies are implementing the Blockchain technology for the systems' quality and working capacity improvement.

Some of the using examples of the Blockchain technology [21], [25], [27]:

- The government management. There are different solutions into the government management. The first decision is Borderless. It is the governance platform which assures the coalition of the legal and economic services [10]. The second solution is the ID2020. This organization is provided proof of the identity for people without documents [13].
- The electronic voting. The Follow My Vote is the secure and transparent platform for anonymous online voting [16]. The E-Residency is the electronic identification system for the citizens of Estonia and for the business-people there [30].
- The authorship. The Ascribe is the platform which confirms and preserves the authorship to the creative people and to the artists. This solution is creating the digital editions with unique ID and the digital certificates for the authorship and authenticity confirming [6].
- The diamonds. The Everledger is the solution which releasing the marker to each diamond for tracking in the connected transactions. This decision helps to solve the real economic, environment and societal problems [15].
- The medicine. The MedRec is the project which provides secure and transparent access to the medical records of each patient in the medical institution [28].
- The supply chains. The Blockverify is the solution for the transparency in the supply chain. This platform has four main using cases: the pharmacy, the diamonds, the luxury items and the electronics [9]. Another example of the solution in the supply chain is the Bext360 which using the Blockchain technology for the coffee trade tracking [35]. The Maersk and IBM corporations are launching the joint venture for the more efficient and secure supply chain with using the Blockchain technology. This platform shows to each participant of the supply chain the products' location and specifications of the transportation [13].

IV. The Blockchain Advantages and Disadvantages

A. The advantages of the Blockchain

The Blockchain technology is decentralized system and it is the main benefit of this technology. Why it is important for our life? The answer to this question is very simple – it is not necessary to work with the third-party organization or with the central administrator. It means that the system works without intermediary and all participants of this Blockchain make the decisions. Each system has the database and it is important to protect this database, because when system is working with the third-party organizations, there is a hacking risk of the database or the data may turn up in the wrong hands. The process of the database security might take a lot of time and might spend a lot of money. If use the Blockchain technology can be avoided, because the transactions of the Blockchain have own proof of validity and authorization to enforce the constraints. And it means that the transactions can be verified and processed independently [1], [36].

Each action is recorded to the Blockchain and the data of records are available to every participant of this Blockchain and cannot be changed or deleted. The results of this recording give the Blockchain's transparency, immutability and trusty [1], [2].

The trusty of the Blockchain is based on the believe of two or more participants, who do not know each other. There is the main idea is the real and not worthless transactions between these unknown people. The trust can be increased further, because there can be more shared processes and records [4], [36].

The immutable is achieved on the transactions are agreed and shared across the Blockchain. When the transaction will be connected to the Blockchain, it won't be possible to change or delete it. It also depends on the system's kind – if the system is centralized, it can be changed or deleted, because the decision is made by one person. But if the system is decentralized, such as the Blockchain, there each transaction, which is joined to the Blockchain, is copied to each computer in this Blockchain network. This benefit makes the Blockchain technology unalterable and indestructible. The users of the Blockchain have empowers to control of all transactions and information. To change or delete the information into the Blockchain is possible when intruder has the fantastic computing power to be able to overwrite or delete the information on the all computers, which includes into the Blockchain before the next block recorded here. If the Blockchain consists of the small number of the computers, the technology is more exposed to be attacked – if there are a lot of computers into the Blockchain than the system becomes safer and more transparent [1], [2], [4], [8], [36].

The transparency of the Blockchain is achieved on the transactions copying process. As it was written above, each transaction is copied to either computer in the Blockchain network. Every participant can look all transactions, also it means, that each action is showed to participants of the Blockchain. Nobody cannot do anything insensibly [4], [8].

The Blockchain designs in a way that it can show any problems and correct them if it is necessary. This advantage makes the Blockchain technology traceability [12].

The high secure of the Blockchain technology is achieved on the individual entry into the network. Because each person who enters the Blockchain is provided with the unique identity which is linked to his account. Another reason of the Blockchain security is the reliable chain of the cryptographic hash. When new block is created, it is necessary to calculate hash value for the new block. The new hash surely includes the previous hash's value. In general, the hash consists of the type, the block's ID number, the previous hash's value, the time when block was created, the user ID number, the miner's level and the merkle root where is stored the information about previous transactions and its hashes. This hash is generated automatically by the node-key. In this case, it is impossible to change any information in the hash value [12].

The multiple ledger causes the clutter and complications to participants of the system. The Blockchain technology is simplification of the ecosystem, because all transactions being added to the single public ledger.

The last one advantage is the faster processing. Traditionally, the transaction takes a lot of time in processing and initialing into banking organization. The using of the Blockchain technology helps to reduce the time for the processing and initialing to many times – from approximately 3 days to several minutes or even seconds [8], [12].

B. The Blockchain disadvantages

If the Blockchain has advantages, this technology has disadvantages or challenges.

The main disadvantage of the Blockchain is the high energy consumption. The consumption of power is needed for keeping a real-time ledger. Every time the new node is created and in the same time it communicates with each and other node. In this way the transparency is created. The network's miners are attempting to solve a lot of solutions per seconds in efforts to validate transactions. They are using substantial amounts of computer power. Every node is giving extreme levels of fault tolerance, ensures zero downtime and is making data stored on the Blockchain forever unchangeable and censorship-resistant. But these actions burning electricity and time – it is wasteful, when each node repeats the achievement of Consensus [8], [36].

The signature verification is the challenge of the Blockchain, because each transaction must be signed with cryptographic scheme, the big computing power is necessary for the calculation process to the sign. It is the one of the reasons to the high energy consumption [8].

The next problem of the Blockchain is the opportunity to split the chain. The nodes, which are operating to the old software, won't accept the transactions in the new chain. This chain is creating with the same history as the chain, which is based on the old software. It is named the fork. There are two fork's kinds – the soft fork and the hard fork [22], [36].

The soft fork establishes the new ruleset to the blocks in the protocol. The nodes are updated to enforce the soft fork's rules. If the block, which was considered valid before, does violate the new soft fork rules, the block won't consider after the soft fork activation. For example, the soft fork is restricting the block size until 500 kB, but before was the 1 MB. It means that the blocks, which are larger than 500 kB, won't be valid in the new chain after upgrades [22], [36].

The hard fork is loosed the ruleset to the blocks in the protocol. This process is the same with the soft fork process, but the value and result of it is the opposite. For example, the hard fork is increasing the block size to 2 MB from 1

MB. If the block is gone through all the rules of the hard fork, the block will be accepted, even if the block was not in the chain before [22], [36].

Another problem of the Blockchain is the balance between the nodes' quantity and the favorable costs for users. Now there are the nodes are lacked for the Blockchain correctly and powerful work. In this case, the costs are higher, because the nodes received higher rewards; but the transactions completed more slowly, because the nodes do not work intensive [36].

The Blockchain has grown when the new blocks affiliate to the chain and the computing requirements increase. Not all nodes can provide with the necessary capacity. There are two problems: the first is the smaller ledger, because the nodes can not carry the full copy of the Blockchain and it breaks the immutability and transparent of the Blockchain; the second is the Blockchain becomes more centralized system [36].

The high costs are a big disadvantage of the Blockchain. The average cost of the transaction is between 75 and 160 dollars and most of it covers by the energy consumption [12]. One of the reasons of this situation has been described above. The second reason is the high initial capital costs of the Blockchain [8].

C. The Attacks and Problems of the Blockchain

The Blockchain can be attacked by the different threats, which are connecting with the PoW and PoS protocols. Most of them are almost impossible [7], [11], [21].

- **Attack of 51%**. It will happen when two miners are calculating the hash of the block at the same time and get the same results. In this case the Blockchain will split and as the result, users have two different chains, and both are considered true.
- **Double-spending**. Princip of this attack is the same with the previous attack, but here can be used the split of the chain to spend the money again.
- **Sybil's attack**. Its possible when one node accepts several essences, because the network can't authentically distinguish the physical machines. The Sybil's attack can help to fill the Blockchain with users under its control. It can lead to the previous two attacks and the ability to see all transactions with special programs.
- **DDos's attack**. The attack consists of a large amount of the similar requests. There is the protection in the DDos's attack – size of the block up to 1 MB, size of each script up to 10000 bytes, up to 20000 of the signatures can check and maximums of the multiple signature is 20 keys.
- **Cracking of the cryptographic**. It is possible if use the quantum algorithms such as 'Shora' which can break the RSA encryption. The scientists work on the cryptographical algorithms, which based on the hash functions.

V. CONCLUSION

The Blockchain is the new type of the database which solved some of the problems in the centralized system, such as the transactions without a middleman, the spent time on each transaction, the unintentional or special deletion or modification of data in the Blockchain.

With the advantages of the technology, such as the transparency, trusty, the multiple copying of the transactions and the decentralized digital ledger, the Blockchain technology is reliable and not destructible, and all mentioned attacks could disrupt the system work, not the technology. It should be noted, that the attacks, which are described in the paper, are more theoretical. There are only few examples of the Blockchain hacking in practice.

The Blockchain technology is useful and versatile for our world, because it can facilitate most of the systems in the different industries, but it is new and it`s implementation is little studied issue on practice. The Blockchain technology promises us the bright future without the fraud and deception due to the benefits of the Blockchain technology. The developers must devote more time to the practical application and implementation of the Blockchain into the already existing systems of the main industrial directions, because the Blockchain can bring the honest and trusty business, government and logistic systems.

The challenges of the Blockchain are large, but the results of the Blockchain using have a greater preponderance than disadvantages.

It is necessary to keep exploring the Blockchain development and application in the different areas for the nearest future, because this new technology can help to solve many difficult problems, which are disturbing and preventing correctly systems work.

REFERENCES

[1] A. Bahga, V. Madisetti, "Blockchain Platform for Industrial Internet of Things", Journal of Software Engineering and Applications, No. 9, pp. [36]533-546, 2016

[2] A. Bahga, V. Madisetti, "Internet of Things: A Hands-On Approach", Atlanta, 2014

[3] A. Litviņenko, A. Āboltiņš, "Computationally Efficient Chaotic Spreading Sequence Selection for Asynchronous DS-CDMA". Electrical, Control and Communication Engineering, vol.13, pp.75-80, 2017

[4] A. Songara, L. Chouhan, "Blockchain: A Decentralized Technique for Securing Internet of Things". Conference paper, October 2017

[5] A. Shanti Bruyn, "Blockchain an introduction. Research paper", 2017. Available from: https://beta.vu.nl/nl/Images/werkstuk-bruyn_tcm235-862258.pdf

[6] Ascribe, "Lock in attribution, securely share and trace where your digital work spreads." [online]. Available from: https://www.ascribe.io/

[7] BitFury Group, "Proof of Stake versus Proof of work. White paper", September 2015

[8] Blockchaintechnology, "Advantages & Disadvantages of Blockchain Technology" [online]. 2016. Available from: https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages-disadvantages/

[9] Blockverify, "Blockchain Based Anti-Counterfeit Solution" [online]. Available from: http://www.blockverify.io/

[10] C. Franko, "Borderless: A Governance Platform and Charity for a Global Society"

[11] D. Balaban, "Blockchain Networks: Possible Attacks and Ways of Protection" [online]. Available from: https://resources.infosecinstitute.com/blockchain-networks-possible-attacks-ways-protection/#gref

[12] Dataflair team, "Advantages and disadvantages of Blockchain Technology" [online]. 2018. Available from: https://data-flair.training/blogs/advantages-and-disadvantages-of-blockchain/

[13] DHL Trend Research, "Blockchain in Logistics", 2018

[14] Ethereum Homestead, "What is Ethereum" [online]. Available from: http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html

[15] Everledger, “Pioneers of digital provenance” [online]. Available from: https://www.everledger.io/about-us/about

[16] Followmyvote.com, “Why Online Voting” [online]. Available from: https://followmyvote.com

[17] G. Nash, ‘What Exactly is Bitcoin?’ [online], June 25, 2017. Available from: https://medium.com/crypto-currently/what-exactly-is-bitcoin-3d5417bff390

[18] H. Kakavand, N. Kost De Sevres, “The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies”, Luther Systems

[19] I. Karamitsos, M. Papadaki, N. Baker Al Barghuthi, “Design of the Blockchain Smart Contract: A Use Case for Real Estate”, Journal of Information Security, No. 9, pp. 177-190, 2018

[20] J. Garzik, BitFury Group, “Public versus Private Blockchains. Part 1: Permissioned Blockchains. White Paper”, October 2015

[21] J. Golosova, A. Romānovs, “Overview of the Blockchain Technology Cases”. In Proceedings of thr 59th Internetional Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), October 10-12, 2018, Riga, Latvia. IEEE, 2018, pp.1-6. ISBN 978-1-7281-0098-2

[22] J.Light, “The differences between a hard fork, a soft fork, and a chain split, and what they mean for the future of bitcoin” [online]. September 2017. Available from: https://medium.com/@lightcoin/the-differences-between-a-hard-fork-a-soft-fork-and-a-chain-split-and-what-they-mean-for-the-769273f358c9

[23] J. Spasavski, P. Eklund, “Proof of Stake Blockchain: Performance and Scalability for Groupware Communications”. Conference paper, November 2017

[24] K. Christidis, M. Devetsikiotis, “Blockchain and Smart Contracts for the Internet of Things”, Special Section on the Plethora of Research in Internet of Things (IoT), May 2016

[25] Lisk, “Government” [online]. Available from: https://lisk.io/academy/blockchain-basics/use-cases/decentralization-in-governments

[26] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, V.Kalyanaraman, “BlockChain Technology: Beyond Bitcoin”, AIR Applied Innovation Review, Issue No.8, June 2016

[27] M. Pilkington, “Blockchain Technology: Principles and Applications”

[28] MedRec, “What is Medrec?” [online]. Available from: https://medrec.media.mit.edu/

[29] P. Gareth, P. Efstathios, “Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money.”, November 2015

[30] Republic of Estonia E-Residency, “The new digital nation” [online]. Available from: https://e-resident.gov.ee/

[31] Sumus Team, “Consensus Algorithm for Bigger Blockchain Networks”, April 2018

[32] T. M. Fernández-Caramés, P. Fraga-Lamas, “A Review on the Use of Blockchain for the Internet of Things”. Article, May 2018

[33] TechBlog “Part 2: How Blockchain works” [online], May 29, 2018. Available from: http://shyamtechno.blogspot.com/2018/05/part-2-how-blockchain-works.html

[34] V. Gupta, “A Brief History of Blockchain”, Harvard Business Review, February 2017 [online]. Available from: https://hbr.org/2017/02/a-brief-history-of-blockchain?referral=03759&cm_vc=rr_item_page.bottom

[35] Very, “Top Blockchain Use Cases for Supply Chain Management” [online]. Available from: https://www.verypossible.com/blog/top-blockchain-use-cases-for-supply-chain-management

[36] W. Fauvel, “Blockchain Advantages and Disadvantages” [online]. August 2017. Available from: https://medium.com/nudjed/blockchain-advantage-and-disadvantages-e76dfde3bbc0