# Overview of the Blockchain Technology Cases

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 technology is not very matured yet, but we cannot underestimate its topicality for modern industry and society. When it appeared first, it was most discussed theme in majority of news and scientific portals. The results of the scientific researches show the big perspective of the use of the Blockchain technology in the different industrial areas. The biggest IT companies develop the Blockchain technology solutions free for use in different spheres. Implementation of these solutions show very positive and fruitful results in different areas of economics. In this paper the description of the Blockchain technology and it's implementation is given. Analyzing numerous applications of the Blockchain technology authors decide the benefits and lucks of it with respect to specific of separate industries.**

***Keywords — Blockchain, data transparency, industial application, use cases***

## I. INTRODUCTION

When people talk about Blockchain technology, most of them think about the cryptocurrency, but cryptocurrency not equals to Blockchain, it is just developed based on this technology. The Blockchain technology can be used not only for cryptocurrency, but can be applied to improve the quality of the system in various economics spheres.

The scientists consider that the main advantages of the Blockchain technology are transparency, decentralized network, trusty chain with the truthful data and unalterable and indestructible technology. One of the important moments is that the transactions are copied to each computer which is include in the Blockchain, and it is not necessary to have intermediaries to carry the transactions. The Blockchain has the opportunities, such as: the possibility to create the block with confidential information; to make the users anonymous or open to other members of the chain; and last one is to create new types of the transactions using existing ones [1], [2].

The Blockchain technology is recognized as a revolutionary invention and it's history shows the development of five innovations [2], [31]:

- the first innovation of the Blockchain was the Bitcoin – the experiment of the digital currency;
- the second innovation was the Blockchain technology itself – when the developers understood that the based technology of the Bitcoin could be used for another aims;
- the third innovation was a Smart contract which embodied in the second-generation of the Blockchain technology and called the Ethereum;
- the fourth major innovation is the Proof of Stake, where the data centers are replaced by the complex financial instruments for the similar or even higher degree of security;
- the last one innovation will be the Blockchain scaling – it accelerates the process of the transactions without weakening security.

## II. ABOUT BLOCKCHAIN TECHNOLOGY

### A. The definition of the Blockchain technology

The Blockchain is dispersed and decentralized database which consisting from a constantly growing list of ordered blocks. One of the most popular definition of the Blockchain is developed by Don and Alex Tapscott: "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".

The most important advantages of the Blockchain technology are transparency and multiple copying of the transactions. It is precisely these advantages make the Blockchain technology unchangeable and not destructive [2].

### B. The structure of the Blockchain technology

Since the Blockchain is the global digital ledger where all transactions constitute the Blockchain network – the blocks form a linear sequence and they are added to the chain with the regular intervals [1]. In turn, each block has some fields with information, which is dependent very much of the Blockchain network. One of the variants is show at the TABLE I.

TABLE I. THE STRUCTURE OF THE BLOCK

| Name of the field | Definition | Size |
|---|---|---|
| BLOCK_ID | The unique number of the block | 4 bytes |
| TIME | The time, when the block was created | 4 bytes |
| USER_ID | The unique number of the user, who created the block | 5 bytes |
| LEVEL | The level, at which a miner was at the time of the block creation | 2 bytes |
| SIGN | The sign from (TYPE, BLOCK_ID, PREV_BLOCK_HASH, TIME, | 128-512 bytes |

978-1-7281-0098-2/18/$31.00 ©2018 IEEE

| Name of the field | Definition | Size |
|---|---|---|
| | USER_ID, LEVEL, MRKL_ROOT) – it is created using the node-key | |
| TRANSACTIONS | Transactions | Up to 3 Mb |

Each block contains the cryptographic hash of the previous block – it is one of the reasons why the Blockchain is not hackable. The hash does not contain any information which anybody would change (TABLE I. ) – it means that all hash's information creates automatically. The 'Merkle Root' includes all previous transactions and its hash values.

Another important moment for the reliability of the Blockchain is the 'Timestamp', which contains 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. These messages include the sender's address, the recipient's address, and the value for transfer and the input data for the recipient contract and those send also by EOAs. The sender's private key signs the transactions, the private key and the account password are necessary for sending transactions to other accounts. In turn, the file JSON of the public-private key is created when the new EOA is created. The message is produced by the contract, but the transaction is produced by the EOA [1], [2]. A Fig. 1 shows the Blockchain structure for clarity.

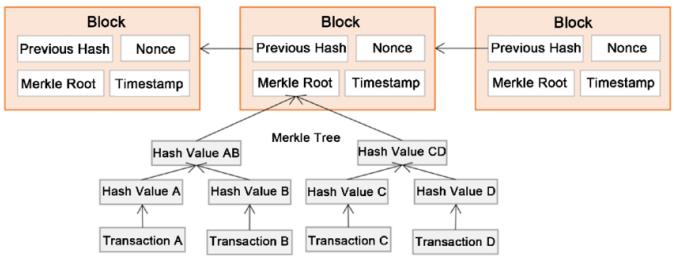


Fig. 1. The structure of the Blockchain [1]

When the Blockchain receive the new block, it checks the block time of the generation, which was indicated by the node. This time includes the time on the generation, on the check and on the wait at the level. 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.

### C. *Access to the Blockchain data*

The Blockchain technology has four varieties, which are classified based on access to the Blockchain data. The TABLE II. shows this classification and the definitions of the classes [18].

TABLE II. THE FIRST CLASSIFICATION OF THE BLOCKCHAIN [18]

| 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 [18].

TABLE III. THE SECOND CLASSIFICATION OF THE BLOCKCHAIN [18]

| 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 |

The financial institutions (such as banks) which use the Blockchain technology in their systems have restricte the direct access. For to ease independent auditing and verifying consistency of the blocks, e.g. by regulatory entities, the financial institutions would [18]:

- to afford the limited read access for their clients;
- to grant the full read access for the regulators;
- to provide the full access with a rigorous and exhausting description of the Blockchain protocol for all entities.

It can help to ease interaction and integration with other Blockchains in the future, because in this case, can speak about the standardized of the Blockchain protocols.

**Permissioned Blockchain**. This category of the Blockchain is intended for the purpose-built and it can be created to maintain compatibility with existing applications. The permissioned blockchain can be fully private or consortium. The transactions of permissioned blockchain won't be on-chain assets; it's mostly will be off-chain assets. The main advantage of these category of the Blockchain is the scalability, because the permissioned blockchain are needed for the smaller preselected participants, they can scale computing power if the number of the transactions will be increased. Some of examples of the permissioned blockchain are Eris, Hyperledger, Ripple [25].

**Permissionless Blockchain**. The verifiers are very important for the Blockchain. Anybody can join to verify in the permissionless blockchain and they participation is encouraged

after that they checked the block 'Proof-of-Work'. The encouragement of participation is necessary for keep the Blockchain safe. The advantage of the permissionless blockchain is the opportunity to can accommodate the anonymous or 'pseudonymous' actors, but it is important to be sure that the verifiers will be encouraged. The biggest of examples of the permissionless blockchain are Bitcoin and Ethereum [25].

### *D. Proof of Work (PoW)*

The Proof of Work is the algorithm of the security of the network relies. The mining is the process of solving a computational challenge imposed by the PoW protocol. To ensure the accuracy of the new attached block, it is necessary to solve a very special mathematical problem. The physically scarce resources, which are needed for the solution of this mathematical task, are [6], [28]:

- specialized hardware for the computations;
- electricity, which is spending to power this hardware.

The PoW protocol is using for the node which wants to participate in mining, in this case the node chooses the block with biggest value of the hash and after that affixes the block to the Blockchain [6], [19], [22].

### *E. Proof of Stake (PoS)*

The minting is the process of solving a computational challenge imposed by the Proof of Stake protocol. It is the alternative to the PoW and this protocol requires far fewer the computations for the mining. The main difference from the PoW protocol is in the calculation, that means the node's balance is proportional to chances of the node mining the next block. In this protocol the trusted entities work together to add records and there is the voting process for accepting the block on the Blockchain [6], [19].

### *F. Smart Contracts*

The smart contract is a part of the Blockchain; more precisely, it is scripts, which are 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], [19]. The Fig. 2 shows the structure of the smart contract.

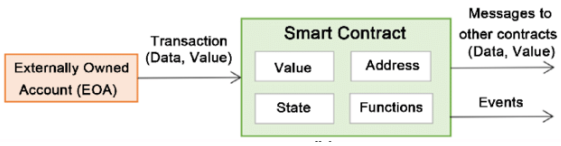


Fig. 2. The structure of the *smart contract [2]*

The behavior of the smart contract is quite predictably, because it proceeds as the autonomous actors. The smart contract also engenders the concept of the 'decentralized autonomous organizations' (DAOs) [1], [2], [19].

### *G. Ethereum*

The Ethereum is adaptable and flexible the Blockchain platform which is open to use it by everyone and programmable. 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) which can help to execute the code of any algorithmic complexity [2], [12], [15].

The Ethereum platform has four processes [17]:

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

## III. THE BLOCKCHAIN TECHNOLOGY CASES

The Blockchain technology is very useful and perspective technology for any industrial and technical area. Now the biggest developers of the IT companies are implementing the Blockchain technology for the improvement the quality and the working capacity of the different systems.

### *A. For the Government and the Private Management*

Some of the examples of the Blockchain technology using into government management [20]:

- *Borderless* – is the governance platform, which provides a big coalition of the legal and the economic services, such as the marriage, the registration of the legal entity, the notary, the financial transactions. These services are based on the smart contracts and the Blockchain *Expanse* [9].
- *Colony* – is the open organization, which can improve the self-organizing companies that run via software. The citizens of the different countries can to create the online-companies, which are based on the Colony platform [3].
- *Boardroom* – is the governance framework and decentralized application, which made to manage smart contracts on the Ethereum for the individuals and the companies. The Boardroom offers the collaborative management of jointly owned digital asset; the organizational decision-making and incentive structures; the industrial consortia project management; the administration of shared digital infrastructure [8].
- *ID2020* – is an organization, which will provide proof of identity to people without some kinds of the documents. This organization uses the Blockchain to share the access with information

about the person without using the paper document. The experts of the ID2020, Accenture and Microsoft corporations will implement the Blockchain solution for the identity of the 7 000 000 refugees from 75 countries by 2020 [11].

### B. The electronic voting

- *Follow My Vote* – is the developer of the secure and transparent platform for anonymous online voting. This solution will can improve the voter turnout, because it is convenient, fast and to be possible for the citizens aboard, the elderly or the disabled to vote. Another advantage of this solution is the cost-effectiveness, because it is not necessary to print out the ballots and to send the information on the emails [14].
- *E-Residency* – is the electronic identification system, which is used by the citizens of the Estonia and the people who have the business interests there. The users of the E-Residency system have the corresponding ID cards and the digital keys to access to wide range of the government, banking and other services [26].

### C. The authorship and the ownership

The Blockchain technology can help to protect the authorship or the ownership to the creative people.

- *Ascribe* – can helps to confirm and preserve the authorship to the creative people and to the artists. The Ascribe allows to create the digital editions with unique identifiers and the digital certificates for the confirm authorship and authenticity. This mechanism which including the legal aspects establishes the transferring ownership from the artist or the author to the buyer or the collector [4].
- *Stampery BTA* – the technology, which can able to process up to $10^9$ data sets/second. It is possible to build the cryptographic tree with all data in real time, because this technology extracts unique secure crypto-identifiers of the processing data. These data can publish into the Bitcoin or the blocks of the Ethereum. The Stampery BTA can helps to integrate own applications or systems with the industrial-scale public API [27].

### D. For the goods and the raw materials

- *The Real Asset Company* – is the next-generation platform for the investments of the gold. This platform is for the gold, silver and other precious metals buyers and provides the online-account for them. The Real Asset Company uses the internal crypto-currency – Goldbloc that adds the complementary level of the transparency to the process of the managing of the gold investments [29].
- *Uphold* – the modern platform for the moving, converting, making the transactions and storing different form of the money, the goods or the raw materials [30].

### E. The diamonds

The diamonds industry is the largest and lucrative branches of the natural extraction. However, there is very high the level of the crime and the violations of the law in this industry. The diamonds are the biggest resources of the financing terrorism. The developers work to solutions, which can help to improve this situation.

- *Everledger* – is the global emerging technology enterprise, which is focused on the real economic, environment and societal problems. The decisions of the solutions are based on the Blockchain technology. In this case, the Everledger releases the marker (such as 'digital passport') for each diamond, which follows it in all connected transactions [13].

### F. For the Medical

Most of the medical centers, which use the electronic systems, do not to distribute the information. This means that the system is the centralized and is incurring the hacking [21].

- MedRec – is the big developer of the solutions with Blockchain technology for the medical institutions. This project is having the aim to provide secure, transparent and scalable access to the medical records [24].

### G. For the Supply Chain

The supply chain is in each area of the world industries. In this case, the Blockchain technology can using anywhere where it is necessary to follow to supply chain from the manufacturer to the customer. Its economies the time, the papers and the financial resources. For the customers this technology can shows the life cycle of the products, that means each participant of the Blockchain can views when and where the products are prepare to the shipment, how it is keep at the shipment and delivery time and other moments [16], [23], [32].

- *Blockverify* – the Blockchain based anti-counterfeit solution for the transparency of the supply chains. The Blockverify has the four main directions in the Blockchain use cases. The first one is the pharmacy – the pharmaceuticals are tracked throughout the supply chain to be sure that customer will receive authentic product. The second case is the diamonds – the diamonds certification is enhancing trust, and this leads to the fraud prevents. The third is the luxury items – this solution is like as the previous (the diamonds), because it helps to provide the quality of the luxury items. The last one case is the electronics – the aim of this solution is to be sure that the customer is getting the original equipment [7].

- *Bext360* is using the Blockchain technology to track the coffee trade. Other developers are engaging the similar systems for the seafood verification and for the food safety [32].
- *Maersk and IBM* are launching the joint venture to use the Blockchain technology for the more efficient and secure of the global supply chain. Each interested participant of the supply chain can follow to the products transportation and knows where the container is now. The paperwork is digitized and automatized and gives to see the status of the different documentation which connected with specific transportation. This platform is piloted by the various famous partners, such as DuPont, Dow, Tetra Pak, Port Houston, the Customs Administration of the Netherlands, and U.S. Customs and Border Protection [11].

## IV. THE BLOCKCHAIN ADVANTAGES AND DISADVANTAGES

### A. *The advantages of the Blockchain*

The main advantage is that the Blockchain is the decentralized system, which does not have one priority person who can controls and makes the decisions. Each action is recorded to the Blockchain and the data of it are available to every participant of this Blockchain. The result of this recording gives the transparency and the trusty of the Blockchain [1], [2].

The second benefit of the Blockchain is the unalterable and indestructible of the technology. It practically is not possible to change or delete the information from the blocks of the Blockchain. To change or delete the information into the Blockchain possible when intruder has the fantastic computing power to be able to overwrite or delete the information on the all computers, which include into the Blockchain before the next block recorded here. That means, 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. Another reason why the Blockchain is unalterable and indestructible technology because the Blockchain uses the cryptographical hash chain. As was mentioned above each block of the Blockchain includes the hash of the previous block [1], [2].

### B. *The Blockchain disadvantages*

The main disadvantage of the Blockchain is the high energy dependence because the mining process consumes the huge power to calculate the hash code of the next block. It is necessary to be the first for getting the remuneration for these calculations. In this case, this bottleneck of the Blockchain limits the high throughput and the low latencies. The parameterization of the block sizes and intervals will not be enough for the biggest load deployments of the Blockchain [1], [2].

Another disadvantage of the Blockchain is the introduction because the financial institutions must abandon their current networks and start to create the new one. The integration can be very difficult process and most of the institutions don't want to implement the Blockchain in their existing systems [1], [2].

All these disadvantages flow into another major limitation – the high costs of the Blockchain implementation.

### 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 [6], [10].

- **Attack of 51%**. It will happen when the 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 be use the split of the chain to spend the money again.
- **Sybil's attack**. It possible when the 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

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. 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.

To the future, developers can think about the systems improvement to increase the advantages of the Blockchain technology and reduce the disadvantages. For example, the

reducing of computing power for the mining process and financial aspect for the Blockchain implementation could be mentioned.

Finally, it is necessary to introduce the practical classes to the educational institutions for the training to build own Blockchain system and to see entire process of the Blockchain technology application and use.

## REFERENCES


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

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

[3] A. Rea, A. Fischer, J. Rose, "Colony. Technical White Paper", 2018

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

[5] B. Dickson, "Blockchain has the potential to revolutionize the supply chain",

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

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

[8] BoardRoom [online]. Available from: http://boardroom.to/

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

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

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

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

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

[14] Followmyvote.com, "Why Online Voting" [online]. Available from: https://followmyvote.com

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

[16] H. M. Kim, M. Laskowski, "Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance", Conference paper, August 2016

[17] 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

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

[19] 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

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

[21] Lisk, "Healthcare" [online]. Available from: https://lisk.io/academy/blockchain-basics/use-cases/blockchain-healthcare

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

[23] M. Pilkington, "Blockchain Technology: Principles and Applications"

[24] MedRec, "What is Medrec?" [online]. Available from: https://medrec.media.mit.edu/

[25] 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

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

[27] Stampery, "Stampery BTA" [online]. Available from: https://stampery.com/tech

[28] Sumus Team, "Consensus Algorithm for Bigger Blockchain Networks", April 2018

[29] The Real Asset Co, "About The Real Asset Co" [online]. Available from: https://therealasset.co.uk/about/

[30] Uphold, "About Us. Passionate About Making the Financial Economy Accessible, Safe and Equitable" [online]. Available from: 32https://uphold.com/en/about-us/company

[31] 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

[32] 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

[33] Y. Guo, C. Liang, "Blockchain application and outlook in the banking industry", Financial Innovation, 2016