Advantages and Disadvantages of Blockchain Technology

Aynesh Sundararaj

Department of Informatics, Technical University of Munich, Germany
aynesh.sundararaj@tum.de

Abstract. Blockchain is one of the very interesting research topics in modern computer science. This report contains a summary of research articles, journals and publications answering various research questions such as What is Blockchain? What are advantages of Blockchain? What are limitations? What are typical applications? What are the different implementations?

Keywords: blockchain, advantages, disadvantages and security.

1 Introduction to Blockchain

Blockchain is one of the trending topics in distributed systems research. Blockchain is basically a consecutive list of blocks which are linked sequentially by cryptography. Blockchain technology provides trust, anonymity and immutability.The data recorded in the blocks are generally tamper proof. Today the Blockchain technology has various applications and its mostly known for it's cryptocurrency implementation called Bitcoin.

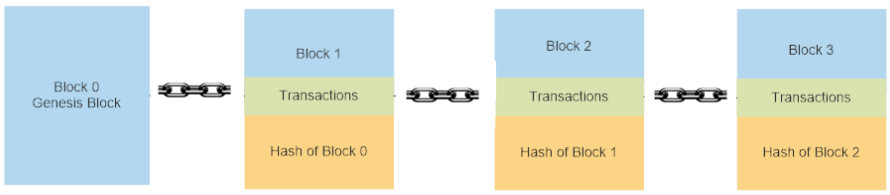

Fig. 1. A block diagram depicting blockchain.

The figure depicts a typical structure of a Blockchain. The arrows describe the link, which is a hash of the previous block. Every block records a cryptographic hash of the previous block. This way the Blockchain ensures that the data is not tampered. Today's Blockchain has many additional features such as Smart contracts etc, which can help you even run small pieces of code on a Blockchain platform.

In the next chapter we talk about building blocks of blockchains, then advantages and disadvantages which is followed by application, examples and conclusion.

2 Building blocks of Blockchain based technologies.

Lets talk about the primary components of a Blockchain. The Blockchain is governed by aspects such as concept of a ledger, the consensus protocol and cryptography[2]. They are the vital components of Blockchain technology.

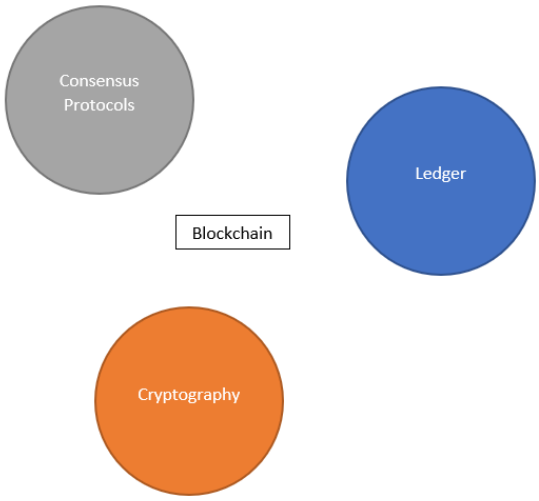

Fig. 2. Building Blocks.

2.1 Ledger

A ledger is a book keeping methodology where you say Alice transferred Bob 10 Euros instead of an account based information. The balance information is inferred by going through the list of transactions. In Bitcoin, a Blockchain is sequence such transactions pooled in to consecutive blocks in a form of linked list. Apart from ledger based book keeping, An account based book keeping is also used. This is implemented in Ethereum.

2.2 Consensus Protocols

A Consensus protocol is basically how multiple parties agree on some value[6]. As we know Blockchain is also a distributed computing. In a Blockchain based

technology the necessity of Consensus protocol comes in when a new block is created. All the participants of the network need to agree if they accept this new block or not. In a normal world, this decision is made by trusted third party. But since the primary goal of Blockchain is to eliminate this third party, we need a method to agree on these new blocks.

Proof of Work In a distributed network someone has to be selected to record the next transaction[12]. We can go for random selection but this will make the network vulnerable. So instead of random selection we present a mathematically hard problem to solve. Whoever solves this hard problem gets to record transaction is allowed to present the next block. This methodology is used in Bitcoin network. The nodes are rewarded for the effort in solving this hard problem.

Proof of Stake In proof of stake, there are validaters instead of miners. The validators have to assign some assert as the stake. This asserts used in real world is some sort of tokens. If the validator thinks that a block belongs to the blockchain, then they can add it to blockchain. If the block gets confirmed the validators get a reward. It's an energy saving alternative to Proof of stake. This algorithm is used in Ethereum cryptocurrency.

Practical byzantine fault tolerance It's a replication algorithm to tolerate Byzantine faults in distributed computing. In each round a new block is created by selecting a node based on some rules. The selected node is allocated to create the next block. The node needs more than 2/3 votes of the network to add the block into the Blockchain. Because of this voting mechanism, only registered nodes can be part of network and voting. This algorithm is used by Hyperledger-Fabric.

2.3 Cryptography

A cryptography is way to hide reading our information by unauthorized persons[16]. The Blockchain is built on Cryptography basics.

- Cryptographic hash functions - These are one way hash functions. Once the message hashed they cannot be reversed to be original form and each message has a unique hash value. This helps in identifying if the information is tampered or not. This is used in linking blocks in Blockchain.
- Public-key cryptography - In public-private-key, the public key is used for encryption, and private or secret key is used for decryption. This system is used to sign transactions in Blockchain based systems.

2.4 Public Private and Consortium Blockchains

Public Blockchains Everyone can participate in the consensus algorithm. Bitcoin is an example.

Private Blockchains It's strictly managed, only approved nodes can participate in consensus algorithm. Ripple is an example for a private Blockchain.

Consortium Blockchains It's partly private Blockchain. Basically its controlled by group of people, but it's shared by multiple organizations. Here the data in the Blockchain can be decided in advance to be public or private. Hyperledger is an example.

3 Advantages and Limitations of Blockchain

3.1 Goals of a Blockchain Technology

The primary goals of a Blockchain was to eliminate the third party based trust. The original use case of a Blockchain was a cryptocurrency called Bitcoin. Many modern goals of Blockchain based technologies evolved from the original use case.

The following below are the primary goals a Blockchain based technology.

- Integrity
- Availability
- Privacy
- Authentication
- Code execution and control.

Integrity Integrity in a Blockchain based system is provided by the long list of immutable blocks. Any tamper to any of the blocks will resulting in a non matching hash of the next block. This way the integrity is ensured. In reality its a combination of technology and incentive based system which streamlines human behaviour to be correct[5]. The major reason being its too costly to rewrite the history.

Availability Blockchain data is maintained in a decentralized manner. Multiple copies of the Blockchain data is maintained by multiple peers in the the network. In this way, the downtime is very less.

Privacy Privacy is provided by pseudo-anonymization. For example in case of a Bitcoin, hash of a Public-Key represents a user in the system. This way the User's identity is not revealed.

Authentication Authentication is provided and controlled by public-private key cryptography.

Code execution and control Code execution and control is provided by the idea of Smart contracts in modern Blockchain based systems.

3.2 Other advantages

No double spending A double spending is an issue, where the same transaction output or Bitcoin is spent on 2 transactions. This is not possible with Blockchain because the next node selecting the new block will identify and select the longest chain. This way the other chain is orphaned and only one chain remains. The figure 3 shows a graphical image of selecting the longest chain.

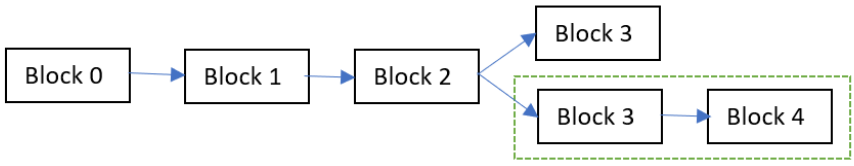

Fig. 3. Selecting the longest chain.

No third party involvement The blocks in blockchain are selected by consensus algorithms, therefore a third party is not necessary.

Anonymity The users of the Blockchain are identified by public-key cryptography. Therefore pseudo-anonymity is ensured. This way the real identity is never revealed. For example the Bitcoin author/organization Satoshi Nakamoto's identity is yet to be known.

Immutable The Blockchain technology is immutable because of its incentive system. When a new block is mined(In case of Bitcoin), there is a mining reward. This mining reward helps the nodes to stay honest. Also rewriting history in a Blockchain is too costly and it outstrips the purpose of rewriting history.

Smart contracts Blockchain provides a mechanism to execute some sort of scripting code in Blockchain platform. In case of bitcoin, it is called Bitcoin script. Using this a user can perform some important steps necessary for executing transactions, eg: preconditions for transactions. Ethereum provides a very highly functional version of smart contracts. More on this will be discussed under Ethereum.

3.3 Limitatations of Blockchain Technologies

High Power Consumption According to research, the main disadvantage of Blockchain technology as high power consumption. They identify the operations

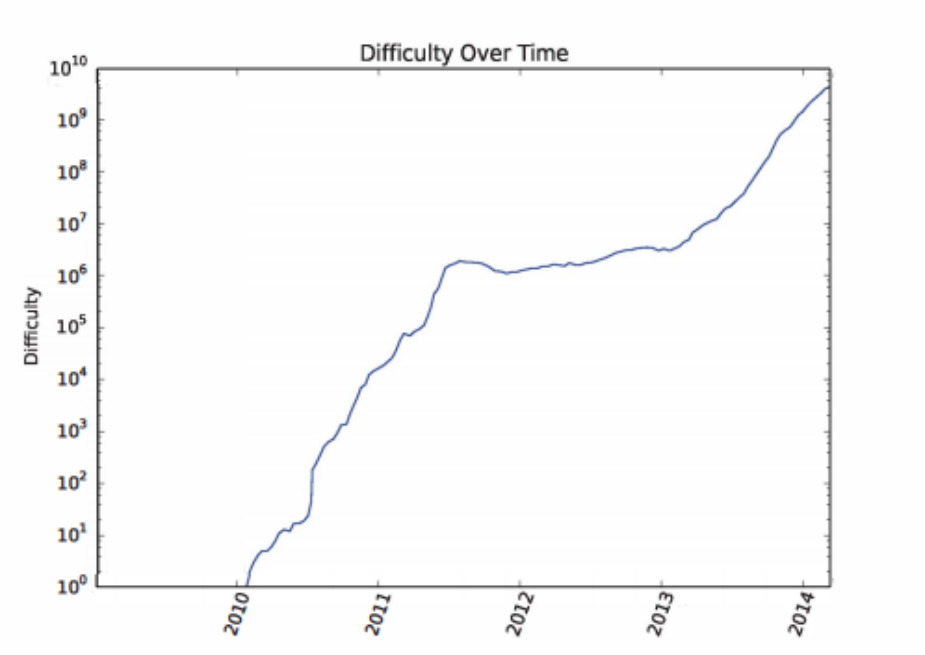

Fig. 4. The difficulty of mining Bitcoin.

that happen in block chain(such as transaction validation) and signing of transactions are the reasons for high power consumption.

From the figure 4 we can see that over the time, The difficulty in mining Bitcoin has increased with time. We can infer the difficulty of mining Bitcoin(Difficulty of solving mining puzzle) is directly proportional to time. We can also correlate that this has led to significant increase in power consumption for mining Bitcoin. This is one of the serious economic drawbacks of Blockchain technology. The research work[11] mentions that the optimization verification of Blockchain can help in reducing of energy consumption some what. The figure 5 shows the increase in power consumption with total number of blocks being mined.

The disadvantage of the possibility of split chains The nodes which run the old version of the Blockchain software will not accept transactions that come from nodes which run the new version of the software. The Blockchain split and this process is called forking. There are two types of fork.

- Hard fork
- Soft fork

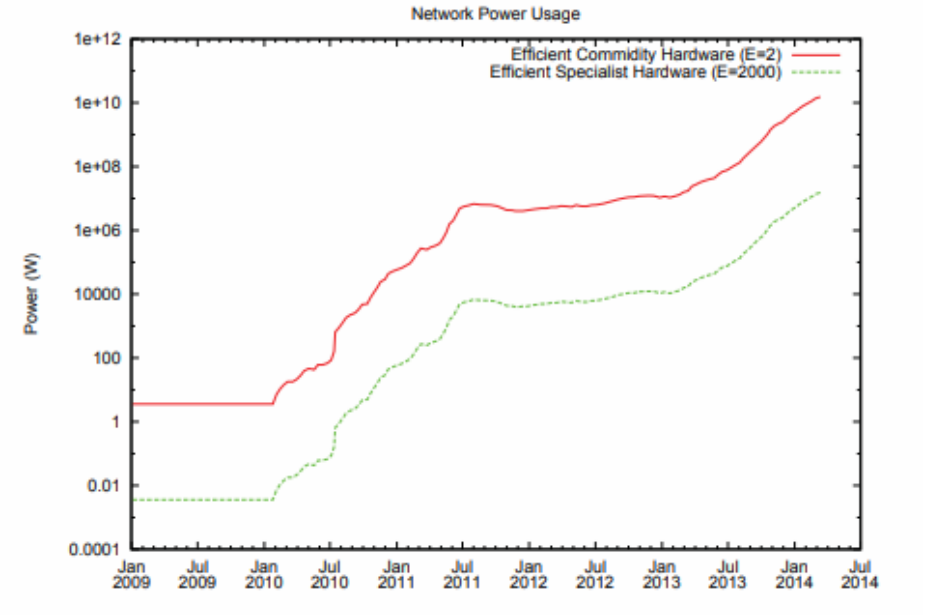

Fig. 5. Estimated power consumption.

Soft folk The soft folk means the new update will not conflict with the current version.

Hard fork Hard fork means the new update will conflict with existing blockchain software and every node in the blockchain networks needs to update to this new version.

The other economic limitation is that that the maintaining higher number of nodes and favourable costs to users. If the number of nodes reduces the blockchain might not perform correctly.

Scaling Scalability is a major issue with Blockchain based technologies. The research work [12] proposes a shared block chains that can be used by many crypto currencies to solve this scalability problem, but the author suspects that getting Blockchains to interact with each other and trusting the mediating Blockchain is an unsolved problem. Also using other consensus algorithms other than proof of work seems to be effective, But for example proof of stake which is another popular consensus algorithm, reintroduces the trust problem again.

3.4 Security threats to Blockchain technology

51 percent attack If the attacker gains more than 51 percent of the network control, the attacker can perform double spending on network. But its not possible to rewrite already written transactions.

DDoss attack The attack consists of a large amount of the similar requests.

Breaking the Cryptography It is shown that encryption algorithms like RSA can be cracked by using quantum algorithms.

Smart contract risks Since you can execute code in smart contracts its vulnerable to attacks. In the article we can see an example for an attack that was carried out using a bug present in the smart contract code[6].

Dependency of transaction order The transactions of block execute in a common shared state data. If 2 consecutive transactions execute, the execution order effects of the output of transactions.

The time stamp dependency The transactions which depend on time stamp present in blockchain is vulnerable since the time stamp data can be changed by the attacker.

Under-Optimized Smart Contract The gas value corresponds to resources in blockchain smart contract execution. This can be exploited by dead code and use of loops.

Selfish mining This attack is performed by hiding the mined blocks without attaching to longest chain by attacker. This attacks goal is waste resources of honest nodes.

The balance attack This attack is targeted at PoW based blockchians. which consists of identifying subgroups of miners with similar mining power and delaying messages passed between them in order to mine blocks before them.

4 Applications

Blockchain can be used to any use cases where we are trying to eliminate to third party trust provider with technology. We will primarily discuss about Supply Chain, Health care and Notary use cases.

4.1 Supply Chain

The supply chain industry faces the issue of counterfeit goods. This can be eliminated by digitization of asserts. This can be achieved with the help of Blockchain.

4.2 Health Care

Health Care has many popular use cases of blockchain. Blockchain can be used to maintain tamper proof patient history and against counterfeit drugs tracking.

4.3 Notary

The paper based records can be digitized with the help Blockchain and can help track changes and records in a tamper proof manner.

5 Technologies

Bitcoin is the most notable and introductory implementation for blokchain. Blockchain in its current form was introduced by Satoshi Nakamoto in his initial Bitcoin draft white paper. Since then many technologies have evolved such as Ethereum, Ripple and Hyperledger.

5.1 Bitcoin

Bitcoint is the first peer to peer version of electronic cash[7]. Bitcoin is the most famous implementation blockchain and its a crypto currency.The Bitcoin was developed based on the shortcomings of current financial systems and necessity for trusting a third party for managing and monitoring financial transactions (Mostly central bank) and how a peer to peer based electronic cash can benefit from such short comings. It's shown that how a peer to peer based electronic cash can function without a trusted third party using blockchain technology and cryptography.

5.2 A Block in a bitcoin

Based on the blockchain technology, underlying fundamental blocks change. For example let's have look at a block of a Bitcoin blockchain(figure 6).

- Block Version - Helps identifying the the blockchain protocol.
- Merkle tree root hash: Is the fingerprint of all transactions in the block. Any modification to transactions will result in change in Merkle tree root hash.
- Timestamp - Timestamp of the block created.
- Nonce: A 4-byte field, which usually starts with 0 and increases for each hash calculation. On receipt of the new block, the complete nodes compute the header hash only once, to see if the Nonce is valid.

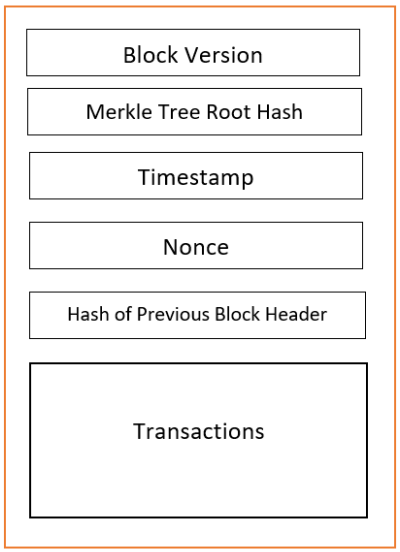

Fig. 6. A bitcoin block.

– Hash of the previous block header - If any the previous block is tampered then the hash won't match. This is how tamper proof property is achieved.

The structure of the block is fundamental to Bitcoin in serving its users. Further the original white paper by Satoshi Nakamoto about Bitcoin showed the bitcoins resistance against security issues such as 51 percent attack and financial issues like double spending. This was the originally proposed bitcoin version and we must note that the bitcoin has gone under several changes since this original proposal.

The principles of blockchain is used in bitcoin are 1) block creation and 2) Adaptation of longest chain. We can see that the transparency benefits of bitcoin is disputable[9], that bitcoin being open source and anyone can join or leave bitcoin network. We also can see that rewards and incentives for participating in bitcoin network and how selfishness of some of the nodes can affect the rewards and incentives schemes. Bitcoin has created a new concept called mining pool, which is an another way to share the rewards in a better way among multiple participating nodes by mining Bitcoin together.

But the idea of mining pool can be dangerous too. Let's discuss the example of CEX.IO. A 51 percent attack is an attack where the attacker has control of more than 51 percent nodes present in the blockchain system and he/she/they can decide which transactions can be included in the blockchain, thereby controlling the entire network. We can also compare between transaction speed of a current Bitcoin system and see how far its behind from standard transaction systems

like Visa and what future holds for bitcoin and blockchains. We can also that there is a problem of growing storage size of bitcoin and limitations caused by 1MB bitcoin size. The network also suffers in case software updates and may lead to hard folks of bitcoin network.

5.3 Ethereum

Ethereum was proposed in late 2013 by Vitalik Buterin. It's a distributed blockchain platform with support for smart contracts. It uses a Proof of Stake as the consensus algorithm. Ethereum uses the concept of gas and world computer. It executes smart contracts in a virtual machine and every execution costs a certain gas. This gas is paid by Ether, which is the cryptocurrency of Ethereum platform.

5.4 Hyperledger

Hyperledger is a group of open source projects developed by linux foundation and supported by big industry players like IBM and SAP. Hyperledger Fabric is the the most popular and notable problem from Hyperledger project group. Hyperledger Fabric is a distributed ledger platform for running smart contracts with various plugins to extend the functionality. It's developed to take blockchains to next level. It uses Byzantine fault tolerance as the consensus algorithm. It is mainly targeting for enterprises and private blockchains.

6 Possible improvements to Blockchain Technology

6.1 Analysis of the possible improvement of Blockchain Technology.

Currently the primary focus is to improve the scalability of blockchains[2]. Let's focus on Bitcoin based networks. We can identify 4 solutions to improve the scalability of Bitcoin based systems.

Segwit Segwit or segregated witness is a mechanism where you isolate the digital signatures from transactions outside the blocks of a bitcoin blockchain. That means you separate verification from transactions, there by you save lot of space. This helps you to include more transactions within the same block. We should also note that around 65 percent block space is occupied digital signatures itself.

Increasing the block size The second solution is increasing the block size. As we know in a bitcoin network, A block is 1MB. Increasing the block size has many positives and negatives. One of the key drawbacks of increasing block size is that full nodes become expensive to operate.

Proof of stake In proof of stake there are validators instead of miners. The validators have to assign some assert as the stake. If the validator thinks that a block belongs to the blockchain then they add it to blockchain. If the block gets confirmed the validators get a reward. The main advantage that, proof of stake consumes considerable amount less energy compared to proof of work. The Ethereum crypto currency uses the proof of stake algorithm called Casper consensus algorithm.

Sharding Sharding in a database world is basically splitting a large database into smaller set of records to maintain the database. The suggestion is to split the blockchain across multiple nodes in the networks. The transactions are split into 2 levels. The first level contains shard-id and a group of transactions. The second level contains the normal blockchain. Its a blockchain first level transaction groups. Each block pointing to one set of transactions. This helps in running parallel transactions. This improves scalability of the blockchain.

6.2 Security improvements

Smart Pool Smart Pool[4] is a a decentralized mining pool. Popular cryptocurrencies have a lot mining pools and they are centralized in nature. Although a joining a centralized mining pool will guarantee some kind of incentive, they are very low and pose a risk of transaction censorship. The authors show how using smart contracts, they can decentralize cryptocurrency mining.

Quantitative Framework Quantitative Framework is proposed a blockchain simulator and security model that mimics blockchain execution and helps to analyze security and performance provisions quantitatively.

Oyente Its a new program proposed by researchers to track errors in smart contracts.

7 Conclusion

In this report I presented summaries of multiple research works in the area of blockchain. Although blockchain has multiple benefits we can understand that it also has some limitations. This has lead to many open research questions and we can see that multiple researchers are working on it. The main objective is to use block chain beyond cryptocurrency.

References

1. Jim Waldo: Hitchhikers Guide Blockchain Universe, Volume 16 Issue 6, November-December 2018 pages 10

2. Daniela Mechkaroska, Vesna Dimitrova and Aleksandra Popovska-Mitrovikj: Analysis of the possibilities for improvement of BlockChain technology. In 26th Telecommunications forum TELFOR 2018, Serbia
3. Sarah Underwood: Blockchain Beyond Bitcoin, Communications of the ACM, November 2016, Vol. 59 No. 11, Pages 15-17
4. S. Sayadi, S. Ben Rejeb and Z. Choukair: "Blockchain Challenges and Security Schemes: A Survey," 2018 Seventh International Conference on Communications and Networking (ComNet), Hammamet, Tunisia, 2018, pp. 1-7.
5. Hanna Halaburda: Economic and Business Dimensions Blockchain Revolution Without the Blockchain in Communications of the ACM, July 2018, Vol. 61 No. 7, Pages 27-29
6. Maurice Herlihy: Blockchains From a Distributed Computing Perspective in Communications of the ACM, February 2019, Vol. 62 No. 2, Pages 78-85
7. Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System
8. Golosova, Julija Romanovs, Andrejs. (2018) : The Advantages and Disadvantages of the Blockchain Technology in 1-6. 10.1109/AIEEE.2018.8592253.
9. Aviv Zohar: Bitcoin: Underthe Hood, Communications of the ACM, September 2015, Vol. 58 No. 9, Pages 104-113
10. K. J. O'Dwyer and D. Malone,: "Bitcoin mining and its energy footprint," 25th IET Irish Signals Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014), Limerick, 2014, pp. 280-285.
11. Bisade Asolo :21 Promising Blockchain Use Cases https://www.mycryptopedia.com/16-promising-blockchain-use-cases/
12. Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukoli, Sharon Weed Cocco, and Jason Yellick: Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference (EuroSys '18). ACM, New York, NY, USA, Article 30, 15 pages.
13. K. Yamashita, Y. Nomura, E. Zhou, B. Pi and S. Jun: Potential Risks of Hyperledger Fabric Smart Contracts, 2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), Hangzhou, China, 2019, pp. 1-10.
14. Boris Sokolov and Anton Kolosov: Comparison of ERP Systems with Blockchain, Platform Intelligent Systems in Cybernetics and Automation Control Theory, Springer pp. 240-248
15. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang: An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017, pp. 557-564.
16. Cryptography Wikipedia: https://en.wikipedia.org/wiki/Cryptography
17. Y. N. Aung and T. Tantidham: Review of Ethereum: Smart home case study, 2017 2nd International Conference on Information Technology (INCIT), Nakhonpathom, 2017, pp. 1-4.
18. Sokolov B., Kolosov A: Comparison of ERP Systems with Blockchain Platform. In: Silhavy R., Silhavy P., Prokopova Z. (eds) Intelligent Systems in Cybernetics and Automation Control Theory. CoMeSySo 2018. Advances in Intelligent Systems and Computing, vol 860. Springer, Cham
19. Yamashita, Kazuhiro Nomura, Yoshihide Zhou, Ence Pi, Bingfeng Jun, Sun: Potential Risks of Hyperledger Fabric Smart Contracts. 1-10.

20. Ethereum Wikipedia: https://en.wikipedia.org/wiki/Ethereum