**Blockchain**

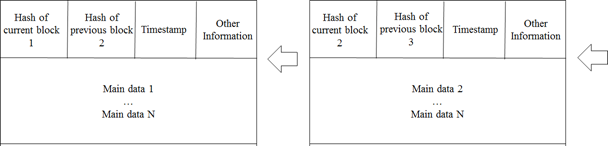
*Md jahidul islam*

*ID:182-15-11497   
Dept. of CSE  
Daffodil International University  
Dhaka, Bangladesh*

**Abstract:** Blockchain advances is quite possibly the most well known issue lately, it has as of now changed individuals' way of life in some space because of its extraordinary effect on numerous business or industry, and what it can do will in any case proceed with cause sway in many spots.Albeit the element of blockchain advances might bring us more solid and helpful administrations, the security issues and difficulties behind this imaginative strategy is additionally a significant theme that we need to concern.

**Keyword:** DLT,Chain,Block,Blockchain,P2P(peer to peer),Bitcoin,Immutable,Ledger, Centralized,decentralized,Noncevalue,proof of work(POW),proof of stake(POS),

**1.Introduction:** For the past couple of years we have reliably heard the term 'blockchain Technology'. The fundamental center of Blockchain Technology is (DLT) Distributed record technology(see Box, Blockchain Glossary)[7][19]. It is an innovative foundation and convention which permits synchronous deciphering, confirmation, and record refreshing in an unchanging nature across an organization that is spread across various elements or locations[13].Nowadays Transactions between two pieces of the world happen in no time. Every one of the recorded exchanges are fixed so nobody can change the exchanges once added to the record. To protect our cash while voyaging we partition cash into various pockets so that regardless of whether a criminal can pickpocketed, He can't take all the cash without a moment's delay. Similarly, in blockchain(DLT), several copies of ledgers are maintained to make changes. The attacker has to hack every node in the network at an equal time which is difficult because an unauthorized change in the ledger will alert other users immediately. Also, all the transactions are counterfeit names, and it is very difficult to track the individuals involved in transactions that provide trust in the system[13].so we can say this technology establishes trust,traceability,accountability and integrity of data sharing.[21]

**Figure 1: Structure of Block chain**

In 2008 satoshi Nakamoto originally concocted 'Bitcoin' which depends on blockchain technology.it is a p2p(peer to peer) Electronic changing out framework. Bitcoin is the decentralized p2p framework which is the main application and it is likewise the most mainstream fruitful execution of blockchain innovation. Blockchain innovation permits advanced data to be recorded and appropriated however not edited.it like a unique kind of database[1][19].it's a computerized cash that permits the clients of the organization to play out the exchange with virtual money that exists just in their PC or processing based gadget securely[6][10].It is likewise the most questionable one since it assists with empowering a multibillion-dollar worldwide market of unknown exchanges with no legislative control[3].People can use blockchain advancements in many fields and administrations, like the monetary market, casting a ballot, IoT, inventory network, clinical treatment, and capacity.Yet, as we utilize these apparatuses or administrations in our regular routine, cybercriminals additionally get a chance to take part in cybercrime and furthermore we can say this innovation is the eventual fate of our humankind[10].

**2.Methodology:** Here we will talk about the functionalities and strategy of Block chain. It is a circulated shared decentralized public record which is open source information design and it is likewise immutable[4].

**2.1 How Block chain Performed:**

|  |  |
| --- | --- |
| 1. | In block chain transduction the sending nood records new data and broadcasts to a network |
| 2. | The receiver nood checked the message from the data which it received,if the given message was correct then it was stored in a block. |
| 3. | All receiving nood in the network use two algorithms one is PoW(Proof of work) or PoS(proof   of Stack) to extract blocks. |
| 4. | Then the block will be stored into the chain by confirming the consensus algorithm,all the    nodes in the network admit that block and it will continuously extend the chain on that block. |

**2.2The Format of Block chain:**

In Figure:1 we have the Structure of BlockChain.In every block we have four Section

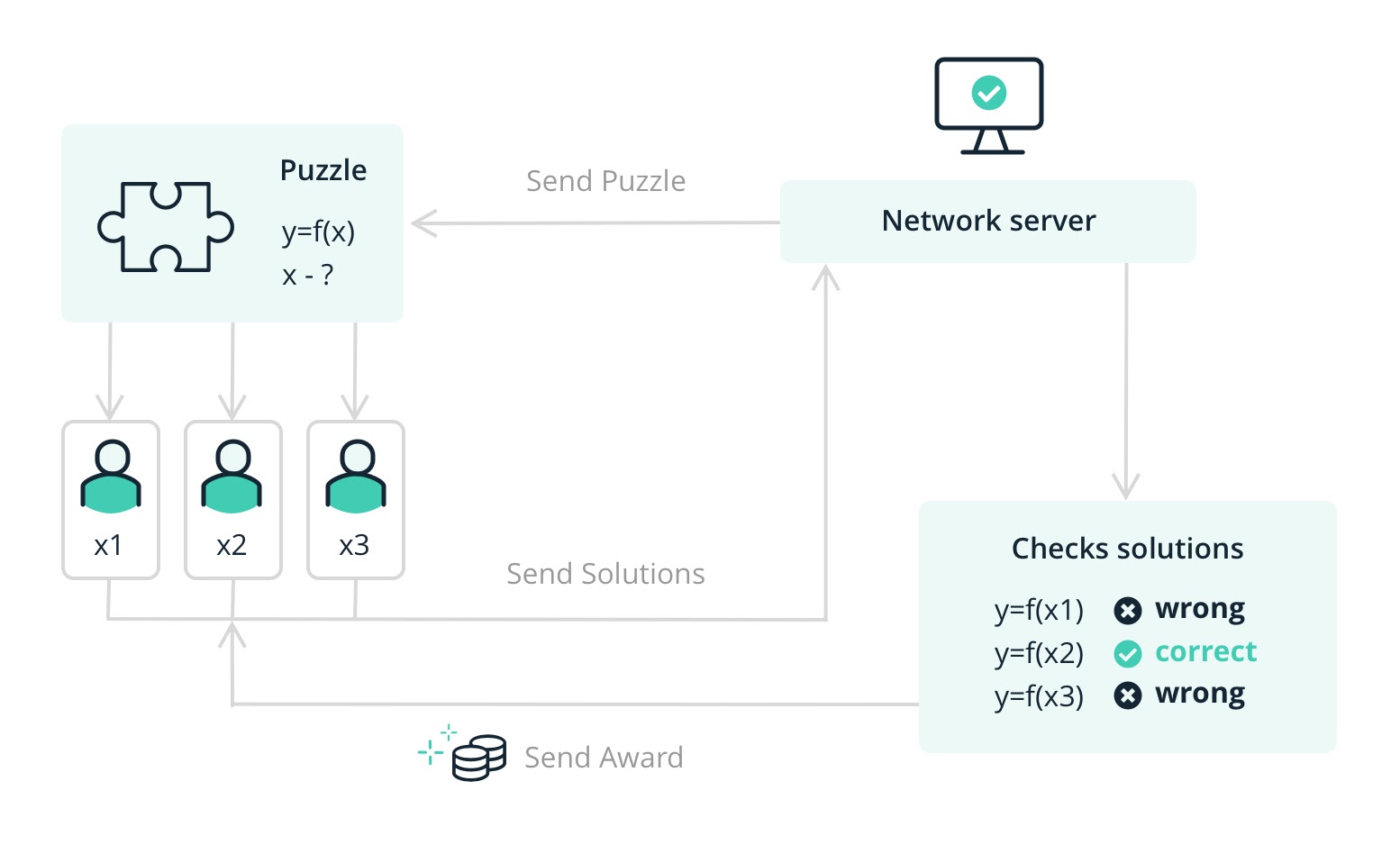
**a.Main data:**In this seasion block contains data depending on what service provides this        blockchain application,like transaction digital currency record,contract records,Bank clearing record.

**b.Hash:**After executing the transaction comes a hash or we can say hashing algorithm.it takes an infinite number of bits then it performs calculations after that it gives a fixed output number of bits. As a result, no matter how long the input is, the output is fixed. Here original data is called input and the final transformation is called hash.

**c.Timestamp:** Every block accommodates a Unix time timestamp. We can say that time stamping is like a digital notary service. Stamping a document on the blockchain proves that the document existed at that particular point in time. Using timestamp we can notarize any media file like txt, pdf, Doc, jpg, etc. So we can say it is the time when a block generates.

**d.Other Information:** It is like a trademark or autograph of a block in the blockchain. It contains a Nonce value or other data that the admin defines.

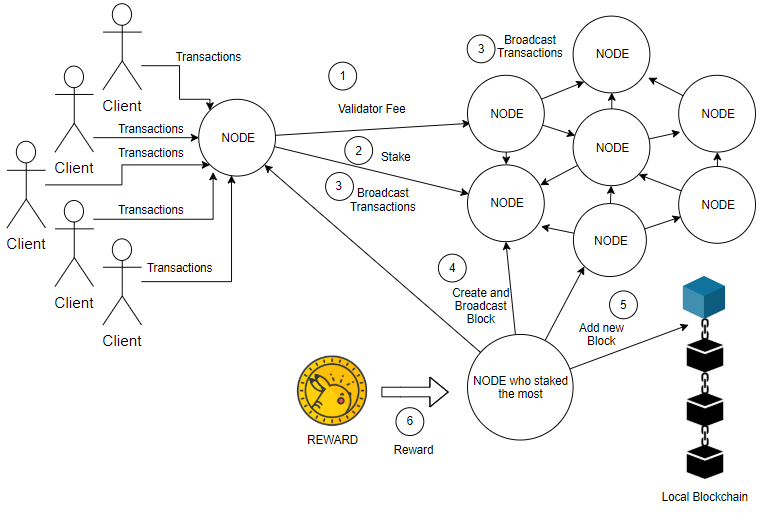
**2.3 Proof of work algorithm(PoW):** Now we will discuss bitcoin for the term of Proof of work. Bitcoin uses a hash cash proof of work system[10]. "Pow" is one of the understanding instruments for delivering concessions to the blockchain network to guarantee exchanges and make another Block to the chain.In the blockchain, every block has an aimless value which is called ‘Nonce’ in Blockheader. “Pow” changes this nonce value, And it also has to generate a value that creates the block header hash value less than 'Difficult Target', Which has already been set. Then we calculate Proof of Work. It is called ‘Mining' .And those people who complete this process are called miners. Miners are part of a community, Who solve the calculation of Pow to produce the upcoming block and broadcast it to the network. And it Produced every 10 minutes. By solving this calculation miners win some reward from both of the blocks (like 10.5 BTC)and the transaction fees in the block[10][19][22].

****

**Figure 2: Proof of Work**

**2.4 Proof of Stack algorithm(PoS):**

By utilizing the 'Proof of work' calculation, mining new coins takes a great deal of figuring power. for a superior alternative In 2011 a client of the bitcoin-talk name Quantum Mechanic proposed a procedure that he called 'Proof of stake'. The basic idea is that letting everyone compete against each other with mining is wasteful. So instead 'proof of stake' uses an election process in which one node is randomly chosen to validate the next block and it also has a small difference in terminology.'Proof of stake' has no miner but instead has 'validators' and it doesn't let people 'mine' blocks but instead 'mine' or 'forge' blocks. validators aren't chosen completely randomly, to become a validator a node has to deposit a certain amount of coins into this network as stake.



**Figure 3: Proof of Stake**

Proof of stake (PoS) is an accord algorithm that decides who legalizes the next block. Depending on how many coins we hold, as a replacement for miners cracking cryptographic puzzles using computing power to justify transactions like they do with traditional PoW(proof of work).

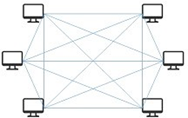
**Table1: Proof of Stake Vs Proof of work**

|  |  |
| --- | --- |
| **Proof of Stack** | **Proof of Work** |
| 1. Echo-friendly, minimal assets needed to get the blockchain. | 1.Power hungry,enough energy to control a little nation is needed to get the blockchain. |
| 2.Truly decentralized stacking(mining). | 2. incentivizes specialized information required. |
| 3. Very little technical knowledge is needed. | 3. Advanced specialized information required. |
| 4.set it and fail to remember it. | 4. Requires steady tweaking and observing. |

**2.4 Classification of Blockchain:**

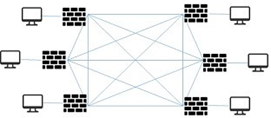
There are 4 types of well known Blockchain:

**1.Public Blockchain:** This Blockchain is public and also decentralized. Everyone can see the transaction, also participants in the process of getting consensus. Example: Bitcoin, Ethereum[10].



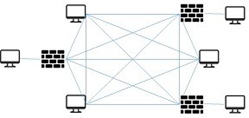
**Figure 4: Public Blockchain**

**2.Private Blockchain:**In private blockchain nodes are restricted and also every node can not participate in the blockchain. It's like a closed network or other that is under the control of a single entity[10].



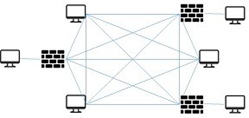
**Figure 5: private Blockchain**

**3.Consortium Blockchain:**It is also known as 'federated blockchain'. This type of Blockchain has public and private blockchain features[10].



**Figure 6: Consortium Blockchain**

**4.Hybrid Blockchain:**It's a hybrid chain that is customized by any two or more blockchains.

****

**Figure 7: Hybrid Blockchain**

**Table2: Advantages,Disadvantages and Use cases of Blockchain**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Public**  (Permissionless) | **private**  (Permissioned) | **consortium** | **Hybrid** |
| **Advantages** | +Independence  +Transparency  +Trust | +Access Control  +Performance | +Access Control  +Scalability  +Security | +Access Control  +Performance  +Scalability |
| **Disadvantages** | -Performance  -Scalability  -Security | -Trust  -Auditability | -Transparency | -Transparency  -Upgrading |
| **Use cases** | ~Cryptocurrency  ~Document    Validation | ~Supply Chain  ~Asset Ownership | ~Supply Chain  ~Banking  ~Research | ~Medical Records  ~Real estate |

**Table3: Comparison of some Cryptocurrency:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Bitcoin**  **(BTC)1** | **Bitcoin Cash**  **(BCH)1** | **Ether**  **(ETH)1** | **Litecoin**  **(LTC)1** | **EOS**  **(EOS)3** | **Stellar**  **(XLM)4** | **NEO**  **(NEO)5** |
| **Launch** | 2009 | 2017 | 2015 | 2011 | 2018 | 2014 | 2014 |
| **Circulating**  **Supply** | Less than 17 million | Less than 17 million | Less than 102 million | Less than 58 million | Less than 906 million | Less than 18 billion | 65 million |
| **Maximum Supply** | 21 million | 21 million | No upper limit | 84 million | No upper limit | No upper limit | 100 million |
| **Current mining/Release rate** | 12.5 per block | 12.5 per block | 3 per block | 25 per block | Up to 5% inflation per year | Up to 1% inflation per year | Up to 15 million per year |
| **Transaction per second (maximum)** | 7 | 60 | 20 | 56 | 2800 | 1000 | 1000 |
| **Network** | n/a | n/a | Ethereum | n/a | EOS.IO | Stellar | NEO |
| **Block time (approximate)** | 10 minutes | 10 minutes | 15 seconds | 2 minutes 30 second | 0.5 seconds | 5 second | 15 second |

**Table4:Comparison of cryptocurrencies with mobile banking like VISA and Paypal**

|  |  |  |  |
| --- | --- | --- | --- |
| **Entity** | **Time** | **Mining Process** | **TPS** |
| Paypal | 1998 | - | 193 |
| Visa | 1958 | - | 56000 |
| Bitcoin [23] | 2008 | Proof of work | 7 |
| Etherium[24] | 2014 | Proof of work | 25 |
| Etherium Casper [29] | 2017 | Hybrid Proof of work and proof of stake | 10,000+ |
| Litecoin[13] | 2011 | Proof of work | 56 |
| Ripple[13] | 2014 | Consensus system | 50000 |
| Nano[26] | 2014 | No Mining | 4000\* |
| Hedera Hashgraph [30] | 2016 | No Mining | 10^6\* |
| Dogecoin | 2013 | Proof of work | - |
| IOTA[25] | 2016 | No Mining | 1500\* |
| Radix# | 2017 | No Mining | 4000\* |
| Bitcoin+Lightning# [28] | 2018 | Proof of work | 10^6 |

Here,

        # = Yet to be released to the  public.

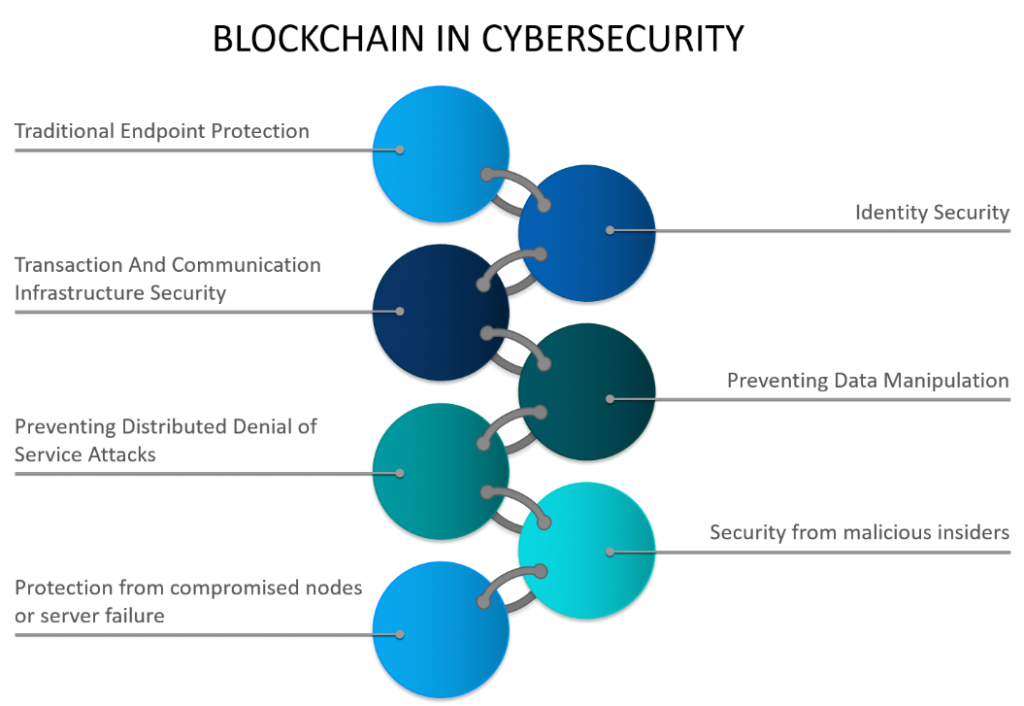
       \* =Theoretical Limit is infinite.

**3.Blockchain Applications & Cyber Security:** Blockchain is an innovation that depends on advanced cash to assist with guaranteeing that all exchanges are appropriately overseen and recorded. Yet, what is put away in the blockchain isn't really a monetary unit; It can be kept in any remaining methods of intriguing use. The ascent of this innovation has prompted an upheaval, it is as yet going on, that is changing numerous parts of our local area. This innovation isn't only the premise of a worldwide known digital currency like Bitcoin, it has a high potential to be applied in different circumstances like money and industry (Figure 8). Also, it has propelled new ways like savvy gets, an exceptionally encouraging innovation that can fundamentally increment blockchain relevance.



**Figure 8: Blockchain Application**

Blockchain is a circulated record of computerized records that are available to all PCs running a similar convention. It takes care of the issue of building up trust in a circulation framework. Blockchain makes a circulated stockpiling of time-stepped archives so no element can alter information or timestamps without detection. Distributed records are decentralized to kill the requirement for a focal power or middle person to measure or verify transactions. As a decentralized data set, Blockchain can carry out different applications like following and confirmation of each sort of register, public or private, recognizable proof, property, exchange or any digitized occasion. Because of the basic idea of these applications and the touchy data, security is a significant worry for clients and engineers.



**Figure 9: Blockchain in Cybersecurity**

Specialists at the Cyber ​​Security Lab explore normal blockchain issues and constraints, like intricacy, network size and speed, human mistake, unavoidable security stream, absence of principles and guidelines, as it can prompt shortcomings in execution and security issues. Cyber ​​security labs are among the most widely recognized security issues among blockchain-based applications, for example, protection spills, affectability, versatility, exchange speed, distinguishing proof and productivity.

**4.Conclusion:** There's no question that blockchain is a hot issue as of late, although it has a few points we need to see. A few issues have as of now been improved alongside new strategies created on the application side, getting increasingly experienced and stable**.**

The public authority need to make comparing laws for this innovation, and endeavor should prepared for embrace blockchain advancements, forestalling it brings an excess of effect on current framework.at the point when we appreciate in the upside of blockchain advancements bring to us, in a similar time, we actually need to remain wary on its impact and security gives that it could be have.

**Reference:**

[1]Cao, S., Cao, Y., Wang, X. and Lu, Y., 2017. A review of researches on blockchain. In *Wuhan International Conference on e-Business*. Association For Information Systems.

[2]Nofer, Michael, Peter Gomber, Oliver Hinz, and Dirk Schiereck. "Blockchain." *Business & Information Systems Engineering* 59, no. 3 (2017): 183-187.

[3]Crosby M, Pattanayak P, Verma S, Kalyanaraman V. Blockchain technology: Beyond bitcoin. Applied Innovation. 2016 Jun;2(6-10):71.

[4]Shah, Tejal, and Shalilak Jani. "Applications of blockchain technology in banking & finance." *Parul CUniversity, Vadodara, India* (2018).

[5]Dewey, Josias N., Robert Hill, and Rebecca Plasencia. "Blockchain and 5G-enabled Internet of Things (IoT) will redefine supply chains and trade finance." In *Proc. Secured Lender*, pp. 43-45. 2018.

[6]Foroglou, George, and Anna-Lali Tsilidou. "Further applications of the blockchain." In *12th student conference on managerial science and technology*, pp. 1-8. 2015.

[7]Rennock, Michael JW, Alan Cohn, and Jared R. Butcher. "Blockchain technology and regulatory investigations." *The Journal* 1 (2018): 35-45.

[8]Cyran MA. Blockchain as a foundation for sharing healthcare data. Blockchain in Healthcare Today. 2018 Mar 23;1:1-6.

[9]Clauson, Kevin A., Elizabeth A. Breeden, Cameron Davidson, and Timothy K. Mackey. "Leveraging blockchain technology to enhance supply chain management in healthcare: an exploration of challenges and opportunities in the health supply chain." *Blockchain in healthcare today* 1, no. 3 (2018): 1-12.

[10]Lin, I.C. and Liao, T.C., 2017. A survey of blockchain security issues and challenges. *IJ Network Security*, *19*(5), pp.653-659.

[11]Vo, H.T., Kundu, A. and Mohania, M.K., 2018, March. Research Directions in Blockchain Data Management and Analytics. In *EDBT* (pp. 445-448).

[12]Zhang, Peng, Jules White, Douglas C. Schmidt, and Gunther Lenz. "Design of blockchain-based apps using familiar software patterns with a healthcare focus." In *Proceedings of the 24th Conference on Pattern Languages of Programs*, pp. 1-14. 2017.

[13]Masood, F. and Faridi, A.R., 2018. An overview of distributed ledger technology and its applications. *Int. J. Comput. Sci. Eng*, *6*(10), pp.422-427.

[14]Bano, S., Al-Bassam, M. and Danezis, G., 2017. The road to scalable blockchain designs. *USENIX; login: magazine*, *42*(4), pp.31-36.

[15]Awan SH, Ahmed S, Nawaz A, Sulaiman S, Zaman K, Ali MY, Najam Z, Imran S. BlockChain with IoT, an emergent routing scheme for smart agriculture. Int. J. Adv. Comput. Sci. Appl. 2020;11(4):420-9.

[16]Litchfield, Alan, and Jeff Herbert. "ReSOLV: Applying cryptocurrency blockchain methods to enable global cross-platform software license validation." *Cryptography* 2, no. 2 (2018): 10.

[17]Zavolokina, L., Zani, N. and Schwabe, G., 2020. Designing for Trust in Blockchain Platforms. *IEEE Transactions on Engineering Management*.

[18]Cachin, C., Sorniotti, M. V., & Weigold, T. (2016). Blockchain, cryptography, and consensus. *IBM Res., Zürich, Switzerland, Tech. Rep*, *2016*.

[19]Welpe, I., Zavolokina, L., Krcmar, H. and Mehrwald, P., 2019. Distributed ledger technology, blockchain minitrack. In *52nd Hawaii International Conference on System Science, Wailea, HI (January 8-January 11, 2019)*.

[20]Seijas, Pablo Lamela, Simon J. Thompson, and Darryl McAdams. "Scripting smart contracts for distributed ledger technology." *IACR Cryptol. ePrint Arch.* 2016 (2016): 1156.

[21]Ribitzky R, Clair JS, Houlding DI, McFarlane CT, Ahier B, Gould M, Flannery HL, Pupo E, Clauson KA. Pragmatic, interdisciplinary perspectives on blockchain and distributed ledger technology: paving the future for healthcare. Blockchain in Healthcare Today. 2018 Mar 23.

[22]Nguyen CT, Hoang DT, Nguyen DN, Niyato D, Nguyen HT, Dutkiewicz E. Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE Access. 2019 Jun 26;7:85727-45.

[23]Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, p.21260.

[24]Wood G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper. 2014 Apr;151(2014):1-32.

[25]Mueller SG, Weiner MW, Thal LJ, Petersen RC, Jack CR, Jagust W, Trojanowski JQ, Toga AW, Beckett L. Ways toward an early diagnosis in Alzheimer’s disease: the Alzheimer’s Disease Neuroimaging Initiative (ADNI). Alzheimer's & Dementia. 2005 Jul 1;1(1):55-66.

[26]LeMahieu, C., 2018. Nano: A feeless distributed cryptocurrency network. *Nano [Online resource]. URL: https://nano. org/en/whitepaper (date of access: 24.03. 2018)*, *16*, p.17.

[27]Masood, Faraz, and Arman Rasool Faridi. "An overview of distributed ledger technology and its applications." *Int. J. Comput. Sci. Eng* 6, no. 10 (2018): 422-427.

[28]Poon, J. and Dryja, T., 2016. The bitcoin lightning network: Scalable off-chain instant payments.

[29]Prashant, B., and I. Makrant. "Migration from POW to POS for Ethereum."

[30]Baird, L., Harmon, M. and Madsen, P., 2018. Hedera: A governing council & public hashgraph network. *The trust layer of the internet, whitepaper*, *1*, pp.1-97.