ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal
Regular Issue, Vol. 9 N. 2 (2020), 91-105
eISSN: 2255-2863
DOI: https://dx.doi.org/10.14201/ADCAIJ20209291105

A Survey on Vulnerabilities and Performance Evaluation Criteria in Blockchain Technology

Devendra Agrawal[a], Anurag Shrivastava[b] and Rishi Kumar Srivastva[c]

[a] Director Academics Goel Institute of Technology & Management Lucknow
[b] Professor and Head, CSE Babu Banarasi Das Northern India Institute of Technology LUCKNOW
[c] Babu Banarasi Das University, Lucknow
dr.devendra@goel.edu.in, headcse@bbdniit.ac.in, rishi.bbdu@gmail.com

KEYWORD

Bloackchain; Bitcoin; Security;Secure

ABSTRACT

The blockchain technology firstly presented by Haber and Stornetta in the year 1990, and first time blockchain technology used in Bitcoin by Satoshi Nakamoto in 2008. The blockchain technology is truly decentralized technology. In blockchain technology, every block has consisted three main parts that is data, hash block, and the previous hash block. Hash is controls the uniqueness of each block and it is unique for each block. Each block also contains the hash of the previous block; thus, the blocks are connected to each other. A blockchain can divided into three categories public blockchain, consortium blockchain and private blockchain. The proposed paper provided the comparative and analytical review on the blockchain consensus algorithms.

1. Introduction

First time blockchain technology was introduced by Haber and Stornetta in year 1990 (Haber et al.1990), and firstly blockchain technology used in Bitcoin by Satoshi Nakamoto in 2008 (Satoshi, 2019). It is a truly decentralized global currency system. Same as any other currency system, the main aim of bitcoin is to simplify the exchange of goods and services by offering a commonly accepted good. In traditional currency system the bitcoin is not issued by a single authority or any state. it did not have common applications. In the current years it has been used in different domains such as supply chain management, biomedical and registering smarts contracts. The group researchers of Casino et al. in year 2019 (Casino et al. 2019) proposed a systematic review on the blockchain application in numerous fields.

Blockchain technology is completely distributed and decentralized database, and in this database consists of is an order of blocks that in each block a transactions list. Every block has three major parts that is data, hash block, and previous hash block. Hash is controls the uniqueness of each block and it is unique for each block. The information of each block is indicated by Hash. When a transaction is registered in a block, its hash number is calculated in an encryption block containing information and is obtained by mathematical rules. Each block contains the hash of the previous block; thus, the blocks are connected to each other. Any changes made in the information of a block cause changes in its hash number. Therefore, any unwanted changes in information of the blocks can cause of alteration in hash number and block become invalid for the other next blocks (Zheng et al. 2019). Following figure 1 is structure of the bitcoin blockchain for the three blocks.

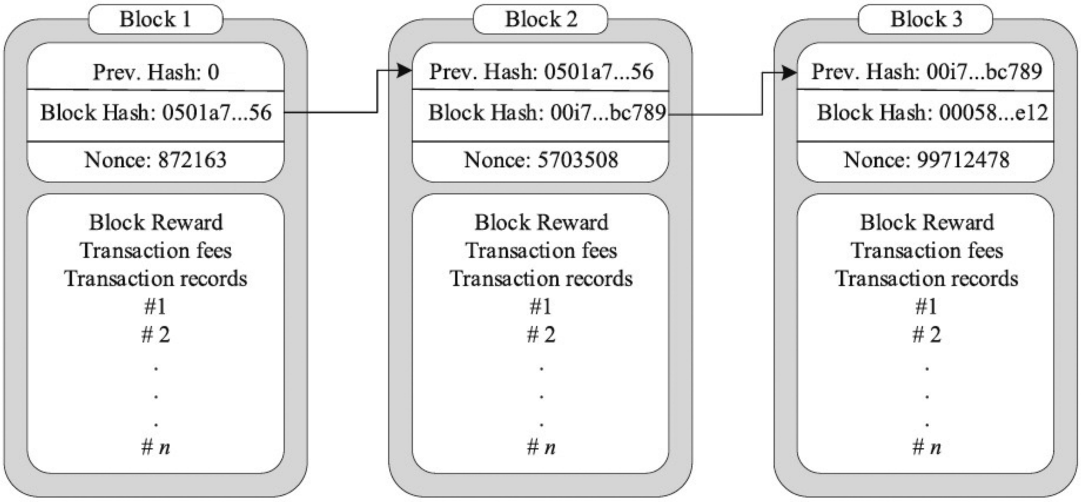

Figure. 1 Structure of bitcoin blockchain for three the blocks.

In the Fig. 1, the block 1 is known as Genesis block and because of there is no any other block before this block, and previous hash amount is zero. Each block can cover thousands of records of transaction that are coded by a hash function before broadcasting to the network. To Generate a final hash value as a hash pointer, blockchain uses Merkle tree function (hash of current block) and each block comprises the hash code of the previous block for the reserve the connection in the blocks.

The Merkle tree is a hash-based type data structure that is a simplification of the hash list. In this tree the leaf node is a hash of block of data, and the non-leaf node is a hash of child node. It reduces the cost of data communication and resources of computing (Panarello et al. 2018). The process of authenticating or mining a new block by the proof of work algorithm is required to do a severely questioning a cryptographic hash function to find a nonce in such a way that satisfies a predefined condition.

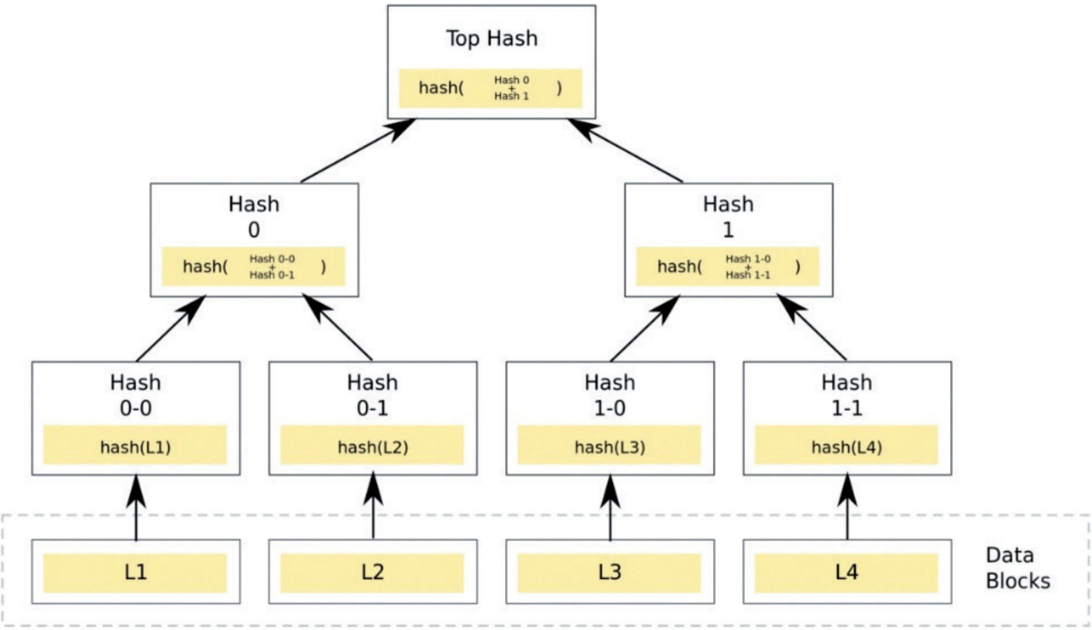

Figure 2: A Hash tree.

Suppose H() is a hash function

x is a Merkle Root of transactions in a block.

Target hash=H(x nonce)≤D(h)

Where nonce= "number only used once" known as added number in hashed block in a blockchain to meet the predefined strain level and for about fixed span of bits L.

$D(h) = 2^{L\text{-}h}$

2. Type of Blockchains

A blockchain is classified into general three categories public blockchain, consortium blockchain and private blockchain (Korpela et al. 2017):

2.1. Public Blockchain

This type of blockchains are measured as a sort of distributed authorization less blockchain in which information is presentable for all network members and all can contribute in its reception. The Bitcoin and Ethereum are the examples of public blockchain. The **Public** blockchains are safe because of its consensus technique achieves contract in the all nodes. Proof of work (PoW) and proof of stake (PoS) are these type of consensus algorithms.

2.2. Consortium Blockchains

Consortium blockchains are also called as federated blockchains. In this chain block the information is reachable to all people, but its change and acceptance is only possible within a certain group. For example, presentation of the marketing products. This type of blockchains are frequently used in banking area (Dib O. et al. 2018).

2.3. Private Blockchains

Private blockchains are type of blockchains in which the data or information is reachable for a distinct group and this blockchain alteration is only possible by an official group. Private blockchains is a centralized blockchain that there is a central expert that make decision on who can write, read or join in the blockchain. Hence in private blockchains the consensus mechanism is control by a single authority.

The main differences in these three types of blockchain algorithm, is how to reach consensus between the peoples. In the public blockchain all miners regulate the consensus, but, in consortium and private blockchain, consensus regulates by a selected group of nodes or by any organization.

3. Blockchain Consensus Algorithm

Please Reaching an agreement in a network of blockchain is a significant and a complex task. The new records of transaction would be added in blockchain since the new block is verified by all nodes in the network.

If once blocks are confirmed, then no once can delete or alter in the blocks. The blockchains structure is designed to be valid in a unreliable and trust less network with argumentative users. There are so many approaches are developed and designed as a consensus algorithm, and these consensus algorithms are increasing day to day. In this part we discuss the various consensus algorithms with the advantages, disadvantage.

3.1. Proof of Work (PoW)

Satoshi Nakomoto (Satoshi N. 2019) introduced the Proof of Work (PoW). It is most well-known consensus technique and it is used in Bitcoins. The Proof of Work has about for numerous years as a appropriate technique for cryptography currency. To solve a mathematics puzzle, the computer system do the calculations. The Hash function is used for solving the puzzle. The Hash is a complex and random mathematical formula that is used for authorization of the transactions stored in the that blocks (Salimitari et al. 2018).

The decentralization and high security are the main advantage of the Proof of Work algorithm. It consumes lot of energy during the mining and validating blocks that is the main disadvantage of that algorithm. Success rate and speed of the hash function vastly depends upon the computational abilities of the hardware running the hash. (Zheng et al. 2017). The complexity is scalable of the hash function, due to the solving the hash functions complexity, it takings some time to solve the puzzle, this proof of work algorithm is not appropriate for large and fast-growing networks that require huge numbers of transactions per second (Alsunaidi et al. 2019).

3.2. Proof of Stake (PoS)

Proof of stake is another common consensus algorithm used in blockchain technology. Major disadvantage of proof of work is it takes lots of energy, for the reason to make proof of stake. This type of algorithm is founded on the idea that the creator of the next block should be chosen by numerous groupings of arbitrary selection, his stake supply, and age which can provide good scalability. PoS algorithm is presented in the Peercoin cryptocurrency in year 2011, after that PoS algorithm also used in NXT and Black coin (Bashir I. 2017). The fast block creation time, energy efficiency, high throughput, scalability (less than PoW) and independence to the special hardware is the main advantage of the PoS based consensus algorithm.

3.3. Delegated Proof of Stake

This delegated proof of stake algorithm was introduced by Daniel Larimer (Larimer D., 2014). This technique is creating by the enhancement of previous blockchain methods. Scalability, low-cost transactions, and low energy consumption are the main advantage of these algorithm. It is semi-centralized algorithm, it used in private blockchains. If any selected representative make a mistake or delay in the performance of the essential reports, the nodes from network can vote to govern to change (Zheng et al., 2017a).

3.4. Practical Byzantine Fault Tolerance

The Byzantine General problem solve in this consensus technique. The malicious attacks on the software have been gradually common. The growing governments and industry on online information services are more attracting the malicious attacks. Errors in software also has been increased due to the complexity of the software and its rising size. Software errors and malicious attacks and can be a result of illogical behavior of faulty nodes.(Castro and Liskov, 1999). In this technique, all nodes necessity to participate in voting process to add next block, and the consensus is reached when more than two-thirds of the nodes have a favorable opinion of the block. In this system with an unwanted node, at least four nodes must have an treaty to reach the correct end, otherwise, the consensus and agreement will not be reached. High throughput and low energy consumption are the advantages of this method and the main disadvantage of this system is there are no parameters available for being scalable and network should wait for all nodes votes.

3.5. Delegated Byzantine Fault Tolerance

This technique follows the rules of Practical Byzantine Fault Tolerance, but the difference is it does not need the contribution of all nodes in the voting process to add a new block. Few nodes are governments the other nodes and, based upon protocols, shadow a consensus process like PBFT method (Salimitari and Chatterjee, 2018). In this technique, few nodes are chosen to record transactions for all the nodes. NEO algorithm uses this type of technique. The Delegated Byzantine Fault Tolerance is less possible to face delays than PBFT but it limits the number of the nodes can portend networks decentralization

3.6. Proof of Weight (PoWeight)

The Proof of Weight associations a wide range of some different type consensus algorithms it is based on Algorand consensus model (Buntinx, 2018). Algor and accomplishes agreement through the byzantine agreement procedure that is able to increases the users according to different parameters and that parameters knowns as weights (Gilad Y. et al. 2017).

In a network of blockchain based upon Proof of Weight, a weight is joined with each user and this weight is calculated by many different factors which would lead to dissimilar consensus algorithms around the proof of weight. These factors are typically based upon how much currency in the users account. Filecoin and Chia cryptocurrencies are the examples of PoWeight.

3.7. Proof of Burn (PoB)

Proof of burn is another technique for reaching a contract in a network of blockchain. The main idea of burn it is that miners or validator no need to waste time or energy to prove. In this type of algorithm, validator or miners have to burn few of already possessed cryptocurrencies to get the rewards. here burning means that a user is mandatory to send some cryptocurrency to the "eater address" to get tokens, coins or mining privileges in the network. The money directed to an address of eater is not recoverable and no anyone can apply it again, so itis known as burnt and is out of circulation. Burning cryptocurrency is an exclusive action for the user there are no consummation of any energy and resources. All cryptocurrencies in PoB require burning proof of work for mine the cryptocurrencies like bitcoin. Cryptocurrency like Slimcoin (SLM) burns bitcoin as a mining technique and consensus algorithm (P4Titan, 2014). The PoB is making more constancy as we know someone who risks a short-term loss and employs his money in this way, would stay in the network for a longer time to gain profits, and there are no factor creating the depositors centralized. PoB algorithm improves decentralization and it also make a distributed network.

3.8. Proof of Capacity

Proof of Capacity (PoC) also called as Proof of Space (PoSpace) and it was introduced in year 2015 by the Dziembowski (Dziembowski, et al. 2015). Here, miners or validators use the free spaces on their storage area to mine free coins. The Burstcoin was the first cryptocurrency based on Proof of Capacity (PoC) and it was founded in year 2014. This type of algorithm contains of plotting the hard drive which means computing and storing solutions on your hard disk before the mining begins. Some solutions are faster than others. If a hard drive transpires to have stored the wildest or closest explanation to the recent puzzle of block, then it wins the block.

Table 1 Comparison of cryptocurrencies based on their consensus algorithm

S. No.	Cryptocurrencies	Consensus Algorithm	Algorithm	Genesis Block	Rank	TPS	Block Time Minutes
1	Bitcoin	POW	SHA256	03Jan 2009	1	07	10
2	Ethereum	POW	Ethash (KECCAK256)	30 July 2015	2	15	0.25

S. No.	Cryptocurrencies	Consensus Algorithm	Algorithm	Genesis Block	Rank	TPS	Block Time Minutes
3	Litecoin	POW	Scrypt	08 Oct 2011	5	28	2.3
4	Monero	POW	Cryptonight	18 April 2014	11	30	02
5	Zcash	POW	Equihash	28 Oct 2016	28	27	02
6	Wave	POS	LPoS	12 June 2016	55	100	1
7	Qtum	POS	POS 3.0	26 Dec 2016	36	70	2
8	NXT	POS	SHA256	24 Nov 2013	175	100	1
9	Blackcoin	POS	Scrypt	24 Fab 2014	500	0	1
10	Nano	POS	Blake2b	29 Fab 2016	45	7000	Instant
11	EOS	DPoS	DPoS	01 July 2017	07	4000	0.5
12	TRON	DPoS	DPoS	28 Aug 2017	13	2000	0.05
13	LISK	DPoS	DPoS	30 Jan 2016	47	03	0.284
14	Ripple	PBFT	N/A	11 April 2013	03	1500	0.06
15	Stellar	PBFT	N/A	06 April 2016	10	1000	0.08
16	Burst	PoC	Shabal256	11 April 2014	190	80	04
17	IOTA	DAG	Curl-P	21 Oct 2015	17	1000	0.08
18	Travelflex	DAG	DAG	02 Dec 2017	1375	3500	1
19	Dash	PoA	X11	19 Jan 2014	16	56	2.5
20	Decred	PoA	BLAKE256	15 Dec 2015	32	14	05
21	Komodo	PoA	Equihash	01 Sep 2016	67	100	1
22	Peercoin	PoA	SHA-256	19 Aug 2012	373	0	10
23	NEO	dBFT	RIPEMD160	17 Oct 2016	20	1000	0.25
24	NEM	PoI	Ed25519	31 March 2015	26	10000	1

4. Vulnerabilities in Blockchain Consensus

Security of the blockchain totally depends upon the strength and robustness of the consensus algorithm that is used to authenticate the blocks and the transactions (Ferrag et al., 2018). There are also many types of vulnerabilities and attacks in blockchain procedures but following are the fundamental and common vulnerabilities (Boireau, 2018).

4.1. 51% attack

Firstly 51% attack was exploited on PoW blockchain network. The 51% attack is not not avoidable problem (Bissias et al. 2016). The protocols in blockchain try to increase the costs of this type of attack to protect it, but they are not able to totally avoid it. When an invader is control 50% power (like authentication or mining power) on the blockchain network. That invader can able to do malicious activities like a double-spending or avoiding other nodes from receiving the true connections. This type of malicious activities is known as 51% attack (Feng et al. 2018). If any attacker does not own 51% of the power of the network then he can offer bribe to the other nodes to follow him or he/she can provisionally rent the power of the network.

4.2. Double spending attack

When a individual attempts to spend a certain amount of money on blockchain twice then the double-spending attack occurs (Zhang and Lee, 2019). When an invader tries to make a normal transaction to contain into a block and then after some time, creates a fraudulent conflicting transaction and impulses it into a new forked fraudulent block, annoying to return the transaction made by him. The invader would try to spread the fake subdivision of network that he has created until the fraudulent branch is verified and accepted as the correct subdivision that includes the fake transaction (Dasgupta et al. 2019). Although different consensus algorithms try to moderate this susceptibility and have a different technique to address it, double-spending fully not avoided in blockchain systems and theoretically it probable to happen all time (Hasanova et al. 2019).

4.3. Sybil attack

Sybil attack is a general form of an attack in which the attacker attempts to control a peer network by creating a number of fake identities in the blockchain (Douceur, 2002). These identifiers appear as different users or locations that actually control the attacker. This identity is used to gain voting power, block credentials, or even to spread a fake message on a blockchain messaging network. A effective Sybil attack gives rites to the attacker a inconsistent control over the network or surround an authentic node and it try to impact the reaching information it and then gradually influence the ledger (Bissias et al., 2016). Sybil attacks are not ease to trace and stop but blockchains attempt to organize their own methods to avoid it.

5. Evaluation Criteria in Consensus algorithms

With the extensive and intensive growth of blockchain technology and its application in different domains, a variety of complex consensus algorithms are developed which have unique, yet diverse properties and applications. The main aim of this proposed review paper is to find the most significant criteria which would affect the performance of these consensus algorithms.

5.1. Throughput

In the current situation in economic system, the customers must be wait for a long time for payment authentication. In current scenario the international transaction completed in up to 3 to 5 days. Due to decentralized and distributed nature of blockchain technology, can make any transaction without the requirement for an intermediary person or bank. This means blockchain technology provides speedy transaction processing and minimal transaction fees. By using consensus algorithms verification of the transactions is completed. Throughput of consensus algorithms, maximum rate of agreement on values in order to verify transaction in a blockchain (Bano et al., 2017). Maximum rate at which the blockchain can completed transactions is known as maximum throughput (Croman et al., 2016), that is a transaction between the maximum block size and the inter-block time. There are many factors that affect throughput of consensus algorithm.

5.2. Transaction per second (TPS)

Transaction per second that is normally used for cryptocurrencies, is known as the number of transactions performed per second. TPS or Transaction per second is the number of transactions that happen in single second through an information system (Shi et al. 2008). The TPS calculation is used to compute the systems performance that handle the repetitive transactions and record-keeping jobs. Transaction per second is used to determine the speed of the platform or network in executing transactions. The large number of TPS (transactions per second), the faster transactions will be executed, and also confirmed and validated on the same platform (Allwein et al. 2001). For example, if any cryptocurrency executs12 transactions in a minute, then TPS for that cryptocurrency is 0.2 (12/60=0.2). The transaction per second is an important factor in blockchain network and depends on its consensus algorithm.

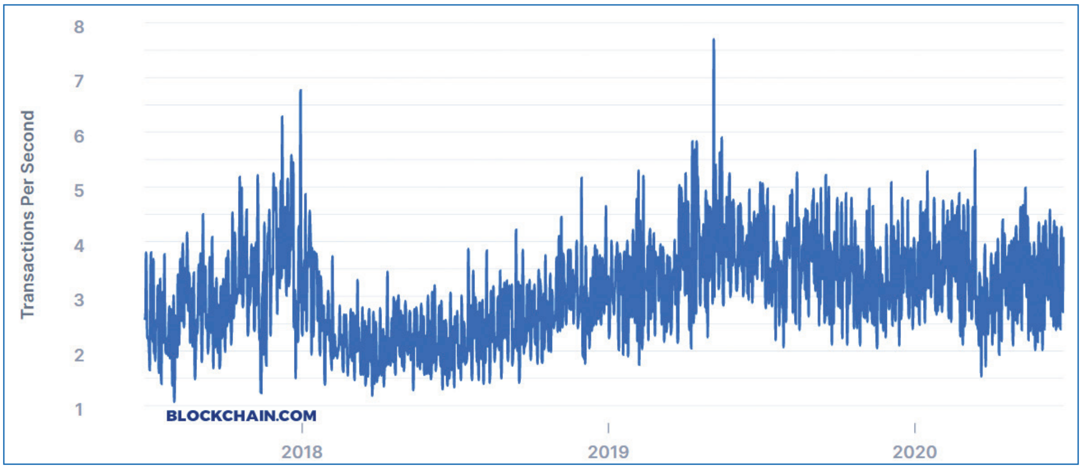

Figure 3: Number of transactions per second.

5.3. Latency of Block Time

Latency or Block time means the delay of authenticating transactions and introducing in a block. Then block is arrived into the blockchain and connected to the existing chain of blocks. It means the latency is the time to takes from when a value is presented to the network, until when a consensus has been reached on it (Bano et al., 2017). As mentioned by (Croman et al. 2016). This is also another important factor that affects the authentication process in network of blockchain named Bootstrap time, which means "the time it takes a new node to download and the process the history essential to authenticate the present system state".

5.4. Block verification time

A transaction between the receiver and sender is known as valid in a the blockchain network if it is requested by sender. When a transaction make by user, he (she) has to use own private key as a digital signature and when a transaction becomes valid, it will be considered as a block and this newly block would be added to the network of blockchain (Vallois and Guenane, 2017).

5.5. Block size

A determined transaction that a block can contain depends on size of block (Zheng, 2017). For some safety reasons block size of bitcoin is limited to 1 MB. If there is no restriction on the block size, some miners can mine a large block, and some other miners mine a small block. This issue damages the network of blockchain. The limited size of block will solve some problem like, due to limited size network is not goes slower. Because of the restriction on the size of block, the verification of the transactions is fast.

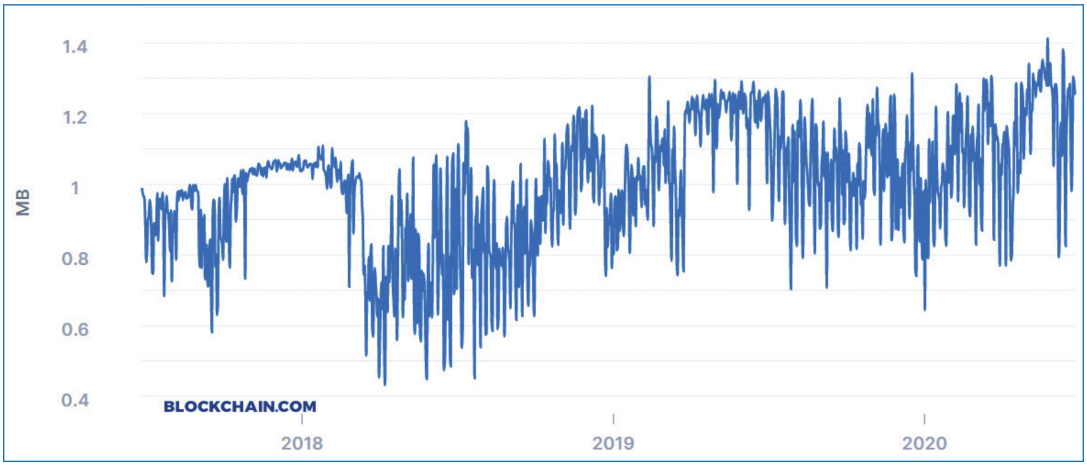

Figure 4: Average block size over the past three years in megabytes.

5.6. Profitability of mining

The profitability of the mining or validation is defined as the total revenue generated by that an authenticator of the blockchain network earn revenue for generating a new block. It comprises giving the technical dimensions for transactions verification and task of network, it resulting in a new block of data on the network. There are different factors that affect the profitability of mining or validation including the difficulty of the process, power consumption, mining rewards, transaction fee and dependency upon the mining process upon specific hardware.

5.7. Mining Rewards

A consensus algorithm is known as procedure to accomplish contract on data's value from among multiple nodes in any distributed systems. In that organizations, in order to obtain security and reliability in that network, the miners or validators are assuming to be employ some kind of computational power, disk space to transactions make authenticate the and also add a new block into the blockchain and in return they receive some rewords. In fact, these types of reward are assumed as an inducement for validator or miners to contribute in the transaction validation process and consequently, the stability of the network is under the assumption that participants behave according to the system incentives (Kroll et al. 2013). Due to nature of the designed algorithms, the validating or mining rewards would change in different blockchains network.

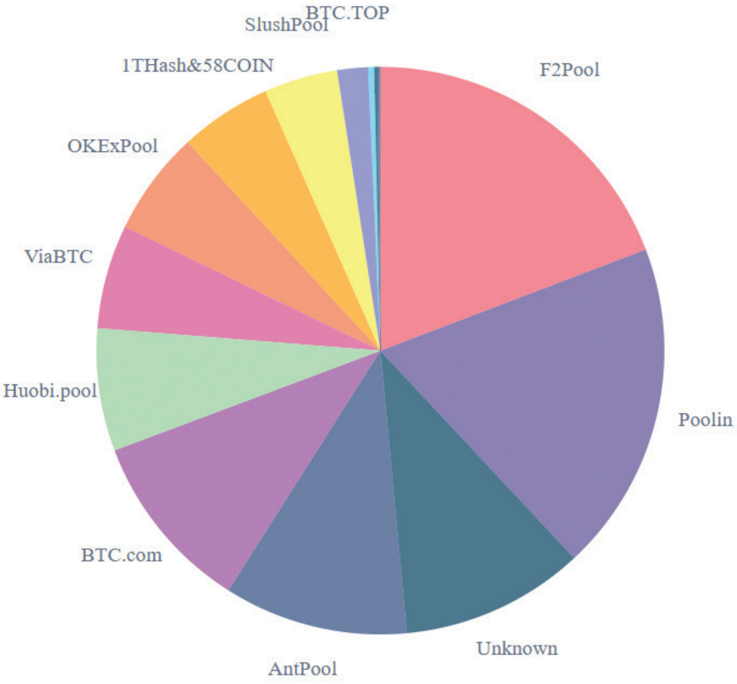

Figure 5. Hashrate Distribution Amongst the largest Mining Pools.

For example, based on the protocol of Bitcoin the mining reward will be shared in every 210,000 blocks. Most of the cryptocurrencies which is based upon PoW algorithms are mineable, while cryptocurrencies based on PoS, PBFT, DPoS and DBFT like Ripple, Stellar, Cardano, NEM, and IOTA are premined and there will be no mining reward in their network. Fig. 5 shows the proportion of hash rate share (the mining power) among the most well-known bitcoin mining pools. As we can see in Fig. 5, most of the amount of mining power is distributed among 13 mining pools. According to the author (Tuwiner, 2020), these mining pools are positioned in a some countries like Czech Republic (10%) and China (81%) and this type of power sharing reductions the decentralization of network of blockchain.

5.8. Power consumption

The power consumption is one of the most significant criteria that affect the calculation of blockchain consensus algorithm. The authors in (Böhme, et al. 2015) stated that the total enrgy taken by bitcoin can give power an to an entire country. This effect is not just about electricity consumption. The main problem is that network of Bitcoin run by power plants which is run by coal in China (digiconomist, 2020). This results in dangerous carbon tracks for each Bitcoin transaction. Energy consumption and performance of some hashing functions like SHA256, SHA512, BLAKE256, RIPEMD160, MD6, and Whirlpool are compared in (Damasevicius 2012).

Although SHA2 family including SHA256, Bitcoin is based on it, is proved to be unbreakable, they are not time competent when it compared to the MD5and SHA1(Kumar Raghuvanshi et al., 2014). The cryptographic hash functions from blake2 series of the which are used in Nano and Siacoin, and it is more secure and faster than MD5, SHA-1, SHA-2 and SHA-3 hash algorithms.

5.9. Transaction fee

The transaction fee is an expense that is pay to the miners to check the block on the system which contains a specific transaction (Tang et al., 2019). Speed of the transaction and fees of transaction are two intently related ideas. In like manner, high-esteem transactions are commonly the speediest. On the off chance that a client has paid a bigger charge, cryptocurrencies forms of miners will organize his/her instalment over others. Fee ordinarily increment as per the developing utilization and fame of cryptocurrencies systems (Zhang, Shi, Tian, & Zhu, 2009). In Fig. 6, the number of transactions of Bitcoin are shown below.

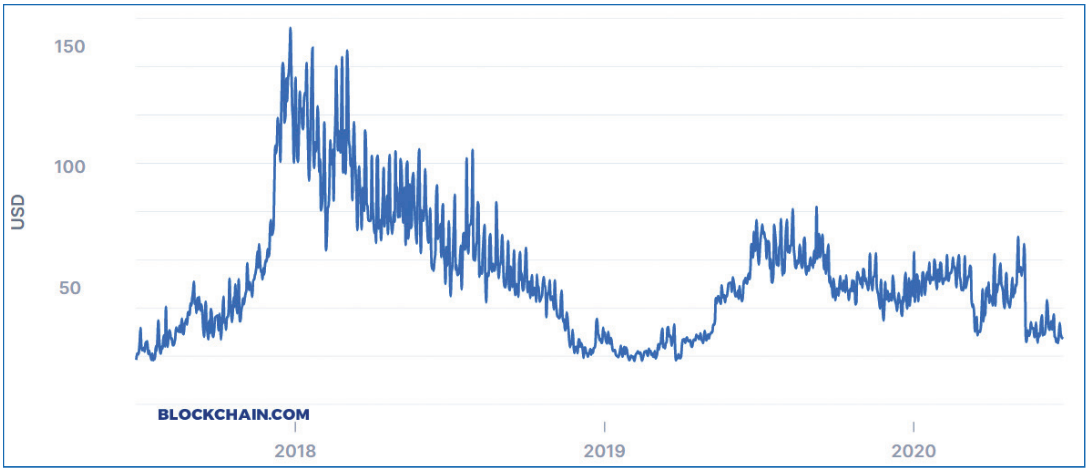

Figure 6: Chart showing miners revenue divided by the number of transactions.

In above Fig. 6 shows the transaction fee, it is an significant part of Bitcoin as an incentive for its validators or miners in simplifying the transactions process but some other type of cryptocurrencies like e.g. Zcahs, ripple, blackcoin, IOTA, that the transaction fee is not necessary and it operate other convincing methods for the miners contribution in the block creation process. It means these type of blockchains use any other type of transaction fees and it gives free user experience.

5.10. Special hardware dependency

The mining process of blocks is meanwhile and highly competitive, the difficulty rate of networks of blockchain is significantly high, so that in determined cases trying to accomplishment this competition without specific hardware called ASIC (application-specific integrated circuit).

In fact, the higher the rate of hash is desired, the longer and more difficult the process would be that is known as the "network hash difficulty". As the hash inconvenience grows exponentially, it needs greater imperativeness, time and resource duty to partake in the mining methodology which is prohibitive for few individual miner.

Few consensus algorithms like dPoS, PoS, and Proof of Authority (PoA) are make for ASIC impervious, and some other algorithms, such as proof of elapsed time this consensus protocol is reliant on specific hardware like Intel SGX and consequently, it stops to take high resource application and more energy consumption. As all of the nodes are mandatory to use definite kind of hardware in this consensus algorithm, the process of mining would remain fair.

6. Conclusion

The blockchain technology is truly distributed and decentralized technology. In blockchain technology, every block has consisted three main parts that is data, hash block, and the previous hash block. Hash is controls the uniqueness of each block and it is unique for each block. Each block also contains the hash of the previous block; thus, the blocks are connected to each other. A blockchain can divided into three categories public blockchain, consortium blockchain and private blockchain. The proposed paper provided the give complete review on vulnerabilities in blockchain technology and various performance evaluation criteria of the consensus algorithms in blockchain technology.

7. References

Alsunaidi, S. J., & Alhaidari, F. A. (2019). Paper presented at the 2019 International Conference on Computer and Information Sciences (ICCIS). A Survey of Consensus Algorithms for Blockchain Technology.

Allwein, E. L., Schapire, R. E., & Singer, Y. (2001). Reducing multiclass to binary: A unifying approach for margin classifiers. The Journal of Machine Learning Re- search, 1, 113–141.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, tech- nology, and governance. Journal of Economic Perspectives, 29 (2), 213–238.

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., et al. (2019). SoK: Consensus in the age of blockchains. In Paper presented at the Proceedings of the 1st ACM Conference on Advances in Financial Technologies

Bashir, I. (2017). Mastering blockchain. Packt Publishing Ltd

Bissias, G., Levine, B.N.,.Ozisik, A.P.,.& Andresen, G. (2016). An analysis of attacks on blockchain consensus. arXiv: 1610.07985.

Boireau, O. (2018). Securing the blockchain against hackers. Network Security, 2018 (1), 8–11.

Buntinx, J. (2018). What Is Proof-of-Weight? Retrieved March 31, 2019, from https: //nulltx.com/what-is- proof- of- weight/#.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics, 36, 55–81.

Castro, M., & Liskov, B. (1999). Practical Byzantine fault tolerance. Paper presented at the OSDI.

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., et al. (2016). On scaling decentralized blockchains. Paper presented at the International Conference on Financial Cryptography and Data Security.

Damasevicius, R., Ziberkas, G., Stuikys, V., & Toldinas, J. (2012). Energy consumption of hash functions. Elektronika ir elektrotechnika, 18 (10), 81–84.

Dasgupta, D., Shrein, J. M., & Gupta, K. D. (2019). A survey of blockchain from secu- rity perspective. Journal of Banking and Financial Technology, 3 (1), 1–17.

Dib, O., Brousmiche, K.-. L., Durand, A., Thea, E., & Hamida, E. B. (2018). Consortium blockchains: Overview, applications and challenges. International Journal On Ad- vances in Telecommunications, 11 (1&2).

Digiconomist. (2020). Bitcoin Energy Consumption Index. Retrieved 16/06/2020 from https://digiconomist.net/BITCOIN- ENERGY- CONSUMPTION.

Douceur, J. R. (2002). The sybil attack. Paper presented at the International workshop on peer-to-peer systems.

Dziembowski, S., Faust, S., Kolmogorov, V., & Pietrzak, K. (2015). Proofs of space. Paper presented at the Annual Cryptology Conference.

Gilad, Y., Hemo, R., Micali, S., Vlachos, G., & Zeldovich, N. (2017). Algorand: Scaling byzantine agreements for cryptocurrencies. In Paper presented at the Proceedings of the 26th Symposium on Operating Systems Principles.

Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2018). A survey on privacy protection in blockchain system. Journal of Network and Computer Applications.

Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Jan- icke, H. (2018). Blockchain technologies for the internet of things: Research is- sues and challenges. IEEE Internet of Things Journal, 6 (2), 2188–2204

Haber, S., & Stornetta, W. S. (1990). How to time-stamp a digital document. Paper presented at the Conference on the Theory and Application of Cryptography.

Hasanova, H., Baek, U. j., Shin, M. g., Cho, K., & Kim, M. S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. Interna- tional Journal of Network Management, 29 (2), e2060.

Korpela, K., Hallikas, J., & Dahlberg, T. (2017). Digital supply chain transformation toward blockchain integration. Paper presented at the proceedings of the 50th Hawaii international conference on system sciences.

Kroll, J. A., Davey, I. C., & Felten, E. W. (2013). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In Paper presented at the Proceedings of WEIS.

Kumar Raghuvanshi, K., Khurana, P., & Bindal, P. (2014). Study and comparative anal- ysis of different hash algorithm. Journal of Engineering Computers & Applied Sci- ences, 3, 1–3.

Larimer, D. (2014). Delegated proof-of-stake (dpos). Bitshare whitepaper, Retrieved March 31, 2019, from https://docs.bitshares.org/bitshares/dpos.html.

P4Titan. (2014). A Peer-to-Peer Crypto-Currency with Proof-of-Burn. Retrieved March 10, 2019, from https://github.com/slimcoin-project/slimcoin-project.github.io/ raw/master/whitepaperSLM.pdf.

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoT integration: A systematic survey. Sensors (Basel), 18 (8). doi: 10.3390/ s18082575.

Salimitari, M., & Chatterjee, M. (2018). An Overview of Blockchain and Consensus Protocols for IoT Networks. arXiv: 1809.05613.

Satoshi Nakamoto (2019). Bitcoin: A peer-to-peer electronic cash system. https://bitcoinsv.io/bitcoin.pdf.

Shi, Y., Peng, Y., Kou, G., & Chen, Z. (2008). Introduction to data mining techniques via multiple criteria optimization approaches and applications. Data Warehous- ing and Mining: Concepts, Methodologies, Tools, and Applications, 3.

Tang, H., Shi, Y., & Dong, P. (2019). Public blockchain evaluation using entropy and TOPSIS. Expert Systems with Applications, 117, 204–210.

Tuwiner, J. (2020). Bitcoin Mining Pools. Retrieved from 18/06/2020 from https:// www.buybitcoinworldwide.com/mining/pools/.

Vallois, V., & Guenane, F. A. (2017). Paper presented at the 2017 1st Cyber Security in Networking Conference (CSNet).

Zhang, D., Shi, Y., Tian, Y., & Zhu, M. (2009). A class of classification and regression methods by multiobjective programming. Frontiers of Computer Science in China, 3 (2), 192–204.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017b). An overview of blockchain technology: Architecture, consensus, and future trends. Paper presented at the 2017 IEEE International Congress on Big Data (BigData Congress).

Zhang, H., Wang, J., & Ding, Y. (2019). Blockchain-based decentralized and secure keyless signature scheme for smart grid. Energy, 180, 955–967.