

International Journal of Computer Science and Mobile Computing



A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IMPACT FACTOR: 7.056

IJCSMC, Vol. 11, Issue. 7, July 2022, pg.8 – 17

A Systematic Analysis on Blockchain Consensus Algorithms and Security Threats

Sonia Rani Chowdhary

Computer Application/DAV University Jalandhar, Jalandhar India

Uic.sonia@gmail.com

DOI: <https://doi.org/10.47760/ijcsmc.2022.v11i07.002>

ABSTRACT- *Blockchain is a new technology which is basically used for store and verified transactions of cryptocurrency like Bitcoin, Ethereum etc. It is a digital, distributed, decentralized and immutable ledger. Transactions in Blockchain always store after verified by multiple validators in peer-to-peer network by using consensus algorithms like Proof of Work (PoW), Proof of Stake (PoS) etc. In blockchain there is no third party involved or managed the transactions. This paper elaborates the basics of Blockchain, its digital transactions in multiple areas like Internet of Things, Education, Manufacturing and financial services, characteristics and limitations of consensus algorithms, gave technical guidance for a suitable consensus algorithms and further areas of research.*

KEYWORDS- *blockchain, cryptocurrency, consensus algorithms, scalability, security threats*

INTRODUCTION- Blockchain generates digital ecosystem in which self-audit transactions are occur. It has main two characteristics transparency and security. A blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a permanent, verified way [1]. The most famous implementations of one being Bitcoin's, created in 2008 by a person or group working under pseudonym "Satoshi Nakamoto" [2]. Bitcoin is a cryptographically secure electronic payment system which is achieved by Timestamping of every transaction in peer-to-peer network and Hashing is used to create chain of transaction blocks. Validators ("miner") are generate new block by using Hashing.

Proof of Work (PoW) is mostly adopted by bitcoin. However, there are many more means to achieve consensus. In Traditional transactions all trusted institutes are centralized, which charges transactional fee, not efficient and secure [4]. Blockchain technology is totally decentralized which solve all these problems. Nodes in blockchain achieve consensus by using predefined protocols. Blockchain technology is actively exploring by all major Banks in the world. To help financial market improve the speed of payment UBS, Deutsche Bank, Bank of Santander and Bank of New York Mellon jointly developed a digital currency system with blockchain technology in Aug 2016. Bank of Santander believe that if all banks in the world use the blockchain, they can save near about \$20 billion every year. The prediction of World Economic Forum is that 10% of the world GDP will be store on the blockchain network by 2027.[3]

LITERATURE REVIEW-

- A. Lloyd’s London presents a report called “Emerging Risk Report 2015” [29] (Beecroft, 2015) and this report discussed different risk factors specifically in Bitcoin. Lloyd’s report studies risk in various domain of Bitcoin such as operational risks, technological risks, market risks and a minor report on security risks in Bitcoin. The Gervais et al. (2016) [30] paper introduced a novel quantitative framework to analyze the security and performance implications of various consensus and network parameters of Proof of Work (PoW) blockchain. Apostolaki , Zohar, and Vanbever (2017) [31] discuss the Bitcoin’s Hijacking. This paper provides a taxonomy of routing attacks and their impact on Bitcoin, considering both small-scale attacks, targeting the network as a whole. Nidhee Rathod, Prof, Dilip Motwani (2018) [17] Discuss the depth of comprehensive survey on blockchain. In this paper present the standard agreement algorithms (PoW, PoS, PoA, PBFT, Ripple, DPoS etc) employed in blockchain and listed some challenges and issues that may hinder blockchain development and summarized some existing approaches for finding these issues.

BLOCKCHAIN OVERVIEW- Blockchain is just like a relational database. It is a public electronic ledger, that is shared by multiple participates and create immutable records which is not modifiable after it is stored.

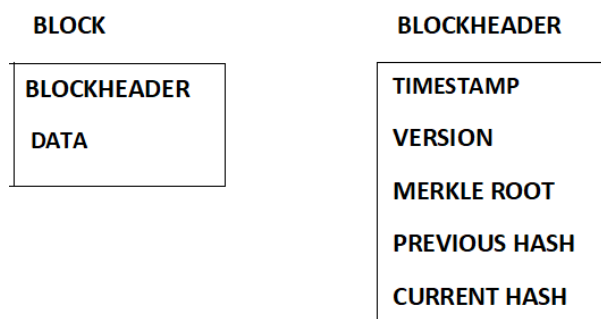


FIG: -1 Block Representation

In blockchain each block contain hash value of current and previous block and first block has no previous hash value and it store by default 0 hash value for previous node or block. If we change any one block data then it effects the next block. If we change one block, we have to change all blocks which are in blockchain. When we create new or updated block it needs to be validate which has some operations and it takes at least 10 minutes to add the block in a blockchain. Each block may contain multiple transactions and each transaction have their own hash value. Multiple hash values of all transactions converted into single hash value of block by using Merkle root.

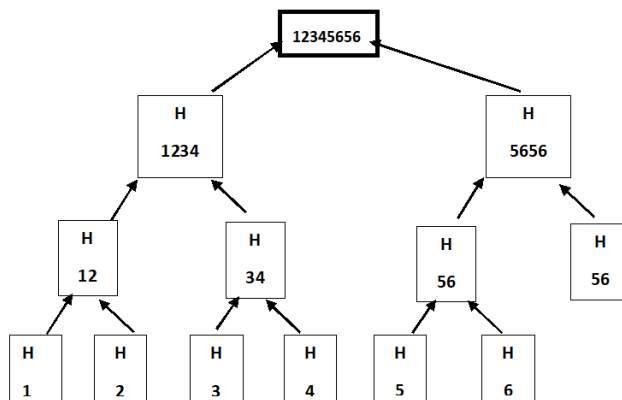


FIG: -2 Merkle Root Generation

WORKING OF BLOCKCHAIN-

Suppose A want to send money to B. Firstly block is created online which represents transaction. Then this block is broadcasted to blockchain network. Block is verified by all the miners of the network by using consensus then added in blockchain and then Money transfer from A to B successfully.

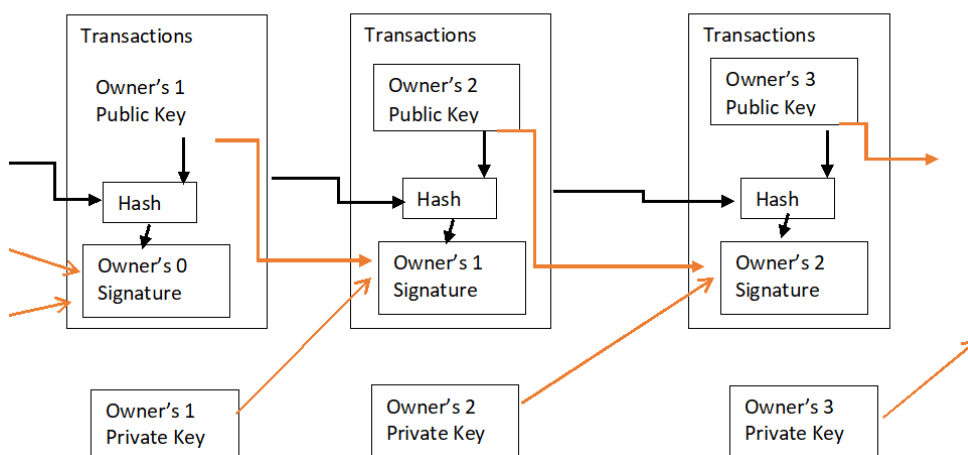


Fig: - 3 Structure of Blockchain

STUDY OF BLOCKCHAIN- It is divided into three categories. Firstly, study on the digital currency that based on Blockchain including the decentralization and centralized currency [5]. Secondly, study on the application of blockchain in smart city [6] and medical information security management [7,8]. Thirdly, study on underlying blockchain technology. Researcher realize that more study needs in blockchain to create revolution in different areas. Some researchers begun study on difficulty in control mining [9], the scalability of consensus algorithm [10] and the smart contract [11].

Table-1: Transactions per second for selected Cryptocurrencies [12]

Cryptocurrency Name	Protocol	TPS
Bitcoin	PoW	7
Ethereum	PoW	15
Ripple	RPCA	1500
Bitcoin cash	PoW	60
Cardano	PoS	7
Stellar	SCP	1000
NEO	DBFT	10000
Litecoin	PoW	56
EOS	DPoS	~millions
NEM	PoI	4000

TYPES OF BLOCKCHAIN- Public Blockchain: Public Blockchain is openly used by all the participates of the network. There is no need of any type of permission. Eg: Bitcoin, Ethereum, Litecoin and many more.

- **Private Blockchain:** Private Blockchain is not open for all. Its read permission may be public or private but write permission is centralized by one organization. In the group of centralized participants are validate the transactions. Eg: MONAX, Multichain.
- **Consortium or federated Blockchain:** It is a special type of private blockchain. Federated blockchain removes the self-auditing or autonomy which is responsible for changes in private blockchain. It is control by group of institutions. Eg: R3(banks), EWF(Energy), and B3i(insurance).

THE CONSENSUS ALGORITHMS-

- Proof of Work (PoW):** Proof of Work is the consensus algorithm basically used in Bitcoin. In PoW algorithm participates should solve some mathematical problem, which is verified by other participates in blockchain network, After the verification of problem new participate can enter into the blockchain network and after doing this new participate get Bitcoin reward through the hashing power competition among the nodes. Satoshi Nakamoto used Hash cash to design the mathematic problems in bitcoin [13].
- Proof of Stake (PoS):** PoS also mentioned in the first Bitcoin project. In PoW Miner is rewarded by solving mathematical problem and create new block but in PoS, the participate of new block is chosen in a deterministic way, depends on its wealth also

define as stake. If participate has no reward coin then miner takes the transaction fee. The earliest application of PoS is PPCoin[14]. Digital currency has concept of coin age. Coin age is a value which is multiply by the time period after it was created. The target amount that a validator needs to contribute in order to mint a new block is determined by the system under the following condition:

$$\text{Proofhash} < \text{coins} * \text{age} * \text{target}$$

- C. Delegated Proof of Stake (DPoS):** In Pos miner gets priority to create new block on the bases of their stake but DPoS is representative democratic. Stakeholder elect their delegates to generate and validate a block [17] then get some reward. Bit share is an eg: of DPoS[18]. DPoS has N number of witnesses participates in the campaign and who get the most of the votes have the accounting rights.
- D. Practical Byzantine Fault Tolerance (PBFT):** The transactional error problem is solved by Byzantine fault tolerance method in distributed system. In starting Byzantine system require exponential operations. In 1999 the PBFT system was proposed and the algorithm complexity was reduced to a polynomial level [20], which is very efficient. It is a replication algorithm. Hyperledger fabric utilize the PBFT as its consensus algorithm since PBFT can handle up to 1/3 malicious byzantine replicas.
- E. Delegated Byzantine Fault Tolerance (DBFT):** DBFT is a variant of BFT. Describe in the NEO whitepaper [21], It split the clients within a P2P system into two separate types: Bookkeeper and ordinary nodes.
Ordinary node does not take part in consensus but vote on which bookkeeper node wishes to support. The bookkeeper nodes which were successfully elected are include in the consensus process. Random bookkeeper node is selected to broadcast its transaction data to network. At least 66% of other bookkeeper should be agree that the data is valid after that transaction is permanently committed to the blockchain.
- F. Ripple Protocol Consensus Algorithm (RPCA):** Ripple Protocol Consensus algorithm is used by Ripple Cryptocurrency [22]and was developed specially to address latency issues present within other algorithms.
RPCA Functions as follows:
- All valid transactions are taken by each server and put it into “candidate set”.
 - All candidate sets are combined by each server in the form of “Unique Node List,” It is a set of other Ripple servers that the server kept reference to.
 - Each server votes on the veracity of each transaction in a series of one or multiple rounds.
 - Minimum 80% of “yes” votes of all transactions can enter in final round and written to the public ledger and the ledger is closed.
- G. Stellar Consensus Protocol (SCP):** SCP is a decentralized consensus protocol [23] which do not need to trust all entire nodes of network but they have ability to choose which nodes they trust. “Quorum slice” concept firstly interduce by SCP, it is a group of nodes which trust each other. A “Quorum” is a set of nodes to sufficient to reach an agreement, whereas a quorum slice is a subset of a quorum which convinces one particular node of agreement. SCP start with candidate value of agreement by “nomination protocol”.

H. Proof of Importance (POI): XEM is an underlying cryptocurrency which is used by Proof of Importance within the NEM network [25]. NEM network account has XEM balance that has two parts: vested and unvested. Whenever an account receives XEM, then new XEM is added to the account’s unvested balance. one tenth of every account’s unvested balance is moved into the vested part every 1440 blocks. XEM maintain the ratio between vested and unvested by taken both vested and unvested balances.

TABLE-2: Consensus algorithm characteristics, Part-1 based on [26]

Algorithm Name					
Property	PoW	PoS	PBFT	DPoS	Ripple
Energy Saving	No	partial	yes	partial	Yes
Tolerated power of adversary	<25%computing power	<51%stake	<33.3% replicas	<51%vliator	<20%faulty

TABLE-3: Consensus algorithm characteristics, Part-2 [26]

Algorithm Name			
Property	DBFT	SCP	Pol
Energy Saving	Yes	Yes	Yes
Tolerated power of adversary	<33.3% replicas	Variable	<50% importance

COMPARISONS OF CONSENSUS ALGORITHMS-

TABLE-4: Comparison of consensus algorithm based on [4]

Characteristics	Consensus Algorithms			
	PoW	PoS	DPoS	PBFT
Byzantine fault tolerance	50%	50%	50%	33%
Crash fault tolerance	50%	50%	50%	33%
Verification speed	>100s	<100s	<100s	<10s
Throughput (TPS)	<100	<1000	<1000	<2000
scalability	strong	strong	strong	Weak

PROSPECTIVE CONSENSUS ALGORITHMS- There are currently numerous alternative protocols that have not yet seen public release. But these are providing the improved form of blockchain.

A. Proof of Luck (PoL): Proof of Luck protocol’s aim to have novel system [27]by reduce the large amount of computational power required by PoW and to increase the transactions throughputs. In PoL each block assigns the “luck” value as it is mined. This value is random number between zero to one. Higher number means luckier and lower means unluckier which is calculated by comparing all the node values of network. A higher luck value has less delay time.

B. **Proof of Exercise (PoX):** Proof of Exercise aims to direct the computing power towards real-world scientific problem. In PoX miner will give the matrix-based problems provided by “employer” within the system [28]. The reason behind using matrices problem is that matrices are composable, allowing for easier tuning of network difficulty, matrices are a principles abstraction for many scientific computational problems. DNA and RNA sequencing, protein structure analysis, datamining, face detection etc provided by the whitepapers.

SECURITY THREATS TO BLOCKCHAIN-

Table-5: Major attacks on blockchain system and its POW based consensus protocols [17]

Attack	Description	Primary Target	Adverse Effects	Possible counter-measures
Double spending or Race attack	Spent the same bitcoins in multiple transactions, send two conflicting transactions in rapid succession	Sellers or merchants	Product drives loosed by sellers, creates block chain forks. , drive away the honest users, create blockchain forks	Inserting observer in network, communicating double spending alerts among peers, nearby peers should notify the merchant about an ongoing double spend as soon as possible, merchant should disable the direct incoming connections
Finney attack	Dishonest miner broadcast a pre-mined block for the purpose of double spending as soon as it receives product from a merchant	Sellers or merchants	Facilitates double spending.	Wait for multi confirmations for transactions.

Brute Force attack	Privately mining on blockchain fork to perform double spending	Sellers or merchants	Facilitates double spending, creates large size blockchain forks	Inserting observer in the network, notify the merchant about an ongoing double spend
Vector76 or one confirmation attack	Combination of the double spending and the Finney attack	Bitcoin exchange services	Facilitates double spending of larger number of bitcoins.	Wait for multi confirmations for transactions.
>50% hash power or Goldfinger	Adversary controls more than > 50% Hash rate	Bitcoin network, miners, Bitcoin exchange centers, and users	Drive away the miners working alone or within small mining pools, weakens consensus protocol.	Inserting observer in the network, communicating double spending alerts among peers, disincentive large mining pools, TwinsCoin, PieceWork.
Block discarding or Self mining	Abuses Bitcoin forking feature to derive an unfair reward	Honest miners (or mining pools)	Interduce race condition by forking, waste the computational power of honest miners, with > 50% it leads to Goldfinger attack.	Zero block technique, timestamp-based techniques such as freshness preferred DECOR+protocol
Block withholding	Miner in a pool submits only PPOWs, but not FPoWs	Honest miners	Waste resources of fellow miners and decreases the pool revenue.	Include only known and trusted miners in pool, dissolve and close a pool when revenue drops from expected, cryptographic commitment schemes.

Fork after withholding (FAW) attack	Improve adverse effects of selfish mining and block with holding attack	Honest miners (or mining pools)	Waste resources of fellow miners and decreases the pool revenue	No practical defense reports so far.
--	---	---------------------------------	---	--------------------------------------

CONCLUSION- Blockchain has different characteristics like decentralization, distributed, security, self-audit, traceable, anonymous, immutable and so on. The most attractive feature of blockchain system is there is no third party involve in two party's transactions. This paper makes review of blockchain basic concepts, its characteristics, consensus algorithms and their comparison, prospective consensus algorithms. Consensus algorithms is a core technology of blockchain. In this paper also summarized the security threats of block chain, challenges in blockchain and some existing approaches for finding these issues. In Blockchain some areas need to be improved like security and privacy of data, size and bandwidth of block, increases the number of transactions and develop more efficient consensus algorithms.

REFERENCES

- [1] M. Iansiti and K. Lakhani, "The Truth About Blockchain", Harvard Business Review, 2018. [Online]. Available: <https://hbr.org/2017/01/the-truth-about-blockchain>.
- [2] S. Nakamoto, "Bitcoin: A Peer-to-peer Electronic Cash System," 2008. [online]. Available: <https://bitcoin.org/bitcoin.pdf>.
- [3] P.Rizzo, "World Economic Forum Survey Projects Blockchain 'Tipping Point' by 2023," , 2015.
- [4] Du. Mingxiao , Ma. Xiaofeng, Zhang Zhe, Wang Xiangwei, Chen Qijun "A Review on Consensus Algorithm of Blockchain", Dept od Control science and engineering, Tongji University, Shanghai, China, 2017.
- [5] G. Danezis and S. Meiklejohn, "Centrally Banked Cryptocurrencies", 2015.
- [6] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in 18th IEEE International Conference on High Performance computing and communications, 14th IEEE International Conference on Smart City and 2nd IEEE Intranational Conference on Data Science and Systems, HPCC/SmartCity/DSS 2016, December 12, 2016 – December 14, 2016, pp. 1392-1393.
- [7] P. T. S. Liu, "Medical record system using blockchain, big data and tokenization," in 18th International Conference on Information and Communications Security, ICICS 2016, November 29, 2016 – December 2, 2016, pp. 254-261.
- [8] Y. Xiao, H. Wang, D. Jin, M. Li, and J. Wei, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control, "Journal of Medical Systems, vol. 40, P.218, 2016.
- [9] D. Kraft, "Difficulty control for blockchain-based consensus systems, "Peer-to-peer Networking and Applications, vol. 9, pp. 397-413, 2016-01-01-2016.
- [10]M. Vukoli, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in IFIP WG 11.4 International Workshop on Open Problems in Network Security, iNetSec 2015, October 29, 2015 – October 29,2015 2016, pp.112-125.
- [11]F. Idelberger, G.Governatori, R. Riveret, and G. Sartor, "Evaluation of Logic-Based Smart Contracts for Blockchain System", Cham, Switzerland, 2016, pp. 167-183.
- [12]L. M.Bach, B. Mihaljevic, and M. Zagar, "Comparative Analysis of Blockchain Consensus Algorithms", Rochester Institute of Technology, Croatia, May,2016.
- [13]A. Back, "Hashcash – A Denial of Service Counter-Measure," in USENIX Technical Conference, 2002.
- [14]S. King and S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake,"2012.
- [15]P. Vasin, "BlackCoin's Proof-of-Stake Protocol v2," Blackcoin.co, 2016. [Online]. Available: <http://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf>
- [16]Nxtwiki, "Whitepaper:Nxt," 2015.

- [17] Nidhee Rathod, Prof, Dilip Motwani, “Security threats on Blockchain and its countermeasures”, Dept. of Computer Engineering, Vidyalankar Institute of Technology, Maharashtra, India, Nov, 2018.
- [18] “<https://bitshares.org/>”.
- [19] “<https://bitshares.org/technology/delegated-proof-of-stake-consensus/>”.
- [20] M. Castro and B. Liskov, “Practical Byzantine fault tolerance,” in Symposium on Operating System Design and Implementation, 1999, pp. 173-186.
- [21] NEO Whitepaper. (2004). Available: <http://docs.neo.org/en-us/>.
- [22] S. David, Y Noah, B. Arthur, The Ripple Protocol Consensus Algorithm, Ripple Labs Inc, 2014. [Online]. Available: https://ripple.com/files/ripple_consensus_whitepaper.pdf.
- [23] D. Mazieres, “The stellar Consensus Protocol: A Federated Model for Internet-Level Consensus,” draft, stellar Development Foundation, 2016. [online]. Available: <https://stellar.org/papers/stellar-consensus-protocol.pdf>.
- [24] L.S. Shankar, M. Sindhu, and M. Sethumadhavan, “Survey of consensus protocols on blockchain applications,” 2017 4th International Conference on Advanced Computing and Communication System (ICACCS), 2017.
- [25] NEM Technical Reference, Version 1.2.2018. [online]. Available: https://nem.io/wp-content/themes/nem/files/NEM_tech_Ref.pdf
- [26] Z. Theng, 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, IEEE, pp. 557-564, 2017.
- [27] M. Milutinovic, W. He, H. Wu and M. Kanwal, “Proof of Luck: An Efficient Blockchain Consensus Protocol,” Proc. 1st Workshop on System Software for Trusted Execution – SysTEX ‘16, 2016.
- [28] Shoker, “Sustainable Blockchain Through Proof of Exercise,” 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), 2017.
- [29] Lloyd’s London presents a report called “Emerging Risk Report 2015”.
- [30] Gervais et al Retrieved February 27, 2018, “Novel quantitative framework to analyze the security and performance implications of various consensus and network parameters of Proof of Work (PoW) blockchain”.
- [31] Apostolaki, Zohar and Vanbever, 2017 “Bitcoin’s Highjacking”.