Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021).
IEEE Xplore Part Number: CFP21ONG-ART; 978-0-7381-1183-4

2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) | 978-1-6654-1960-4/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICICV50876.2021.9388487

Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain

P. Rajitha Nair

Department of Computer Science & Engineering

T John Institute of Technology

Bangalore, India

jstria@gmail.com

Dr. D. Ramya Dorai

Department of Computer Science & Engineering

T John Institute of Technology

Bangalore, India

ramyadorai@tjohngroup.com

Abstract - Storing information in Blockchain has become in vogue in the Technical and Communication Industry with many major players jumping into the bandwagon. Two of the most prominent enablers for Blockchain are "Proof of Work" and "Proof of Stake". Proof of work includes the members solving the complex problem without having a particular need for the solution (except as evidence, of course), which absorbs a large number of resources in turn. The proof of stake doesn't require as many resources to enable Blockchain secure information store. Both methodologies have their advantages and their shortcomings. The article attempts to review the current literature and collate the results of the study to measure the performance of both the methodologies and to arrive at a consensus regarding either or both methodologies to implement Blockchain to store data. Post reviewing the performance aspects and security features of both Proofs of Stake and Proof of Work the reviewer attempts to arrive at a secure and better performing blended Blockchain methodology that has wide industry practical application.

Keywords - Proof of stake, Proof of work, Performance, Security, Merkle Tree, Blockchain, Practical Blockchain, Blended Block chain

1. INTRODUCTION

Blockchains have been suspected as the revolution that will enable money control to move from central organizations like Governments, Centralized Banks and rather become distributed – a true money democracy. However, the key to a centralized data repository is assured data security. An example of an unsecured data store is when one of the participants of the Blockchain publishes a ledger that is advantageous/profitable but which is not real. Since the ledger is distributed the other participants will not be able to ascertain the accuracy of these published entries. This causes the data stored in such a network to be marked as undependable.

1.1 BlockChain Technology

Blockchain is a list of secure linked records that is continuously increasing and allowed by Cryptography [6] [7], or also known as blocks. Along with the hash pointer, the Time-stamp and the Transaction Data connect each block of information to the previous block. The immutability of data is a key attribute of blockchain [8]. Functioning as a distributed ledger Blockchain is accomplished by a peer-to-peer network collaborating with a shared protocol for validation of new information blocks. To alter data, more than 50% of the network is required to give consensus in a given block. Changes in one block require the same data to be edited and saved in all subsequent informational blocks [9].

Blockchains are stable by nature, exemplifying a computer system distributed with exceptional Byzantine fault tolerance [9]. Decentralized consensus has therefore been materialized with a Blockchain which ensures Blockchains are possibly suitable for the recording of events like hospital records, management of identity, processing transaction, the origin of recording, or traceability of food [10].

Satoshi Nakamoto conceptualized the first distributed Blockchain, in 2008 with Bitcoin and non-fiat currency that was digital which serves as the ledger in public across all transactions. This makes the digital currency that resolves the problem of double-spending without a separate reliable authority or server that is centralized [6].

With a stored data that is spread in a self-managed network, Blockchain removes the risks that are part and parcel of data held in a central location. This decentralized Blockchain uses impromptu message passing and networking that is distributed. Network lacks central vulnerable points which can be referred to as points of failure. Blockchain security approaches contain the use of public-key cryptography. A public key (a random-looking string of numbers usually long) is an address on the Blockchain with valued tokens sent across the network recorded in that address. A private key provides its owner access to their digitally held assets or else converse with the various capabilities that Blockchain now support. Data stored on the Blockchain is considered in general as a not corruptible and immutable block of information [12]. A blockchain database consists of two types of records - blocks & transactions [12] [13]. A transaction that is encoded, valid, and hashed from the Blocks in Merkle tree format. Each block has a hash code of the previous block in the Blockchain hence connecting the two hashes linked blocks.

1.2 Merkle Tree

Hash Tree or Merkle tree in cryptography is a tree in which every single leaf node is labelled with a data block and each non-leaf node is re-labelled with the cryptographic hash of the labels of its child nodes. Secure and effective verification of contents of large data structures is permitted by Hash trees which is a generic form of hash chains and also listed.

Several hashes' computation is mandatory to determine that a given binary hash tree has the leaf node. The number of hashes is a function of the logarithm of the number of leaf nodes of the tree. In comparison, the hash lists function remains proportional to the number of leaf nodes itself.

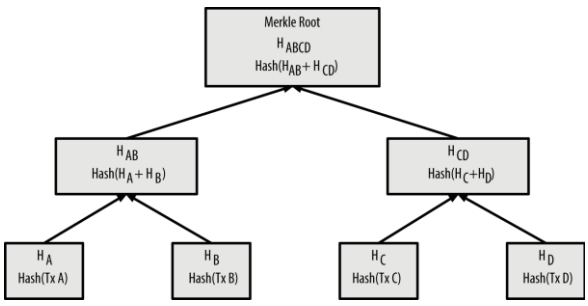

Figure 1: MerkleTree

There are 2 foremost ways in which Blockchain can be executed algorithmically and Distributed Consensus arrived at – Proof of Stake and Proof of Work [14] [15].

1. Proof Of Work

Proof Of Work requires the participants to mine a block requires them to solve an increasingly difficult problem to ensure the mined block is valid [2]. Each of the mined blocks ensures that the miner is rewarded with a certain amount of coins. The algorithm defined may be a function of the number of participants and the current difficulty level of the computational problem.

Proof of Work's major disadvantage is the wastage of resources spent by the miners to mine a new block of information. The wastage is in terms of electricity spent by the miners which taxes not just the miner but also creating pressure on the grid.

.

Computing methods that are used in a way to solve a problem that could have been better used to solve many other scientific, astronomical, and medical problems.

Miners need to keep improving their device and have a continuous power supply to be profitable and this, in turn, ensures that they don't tamper with the ledger. However, if the miners can secure a 51% plus stake they can easily tamper the blockchains and hence make them insecure. For example, one of the major assumptions of Bitcoin is that "the majority of the miners are fair". However, this is not something that is provable and is rather an assumption.

2. Proof Of Stake

On the other side, Proof of Stake works by providing the user who has the highest stakes in each network with the opportunity to exploit. Having the highest stakes gives the miner credibility and assurance that he will not tamper with the ledger. Having the highest (or higher than most) stake makes the miner want to maintain the credibility of the ledger and hence avoid fraudulent transactions. Proof of Stake mechanisms have been proven as not scalable and hence more suitable for a private network setup and cannot be effectively adopted for large scale use cases.

2. Proof Of Work Performance

Rong and Wai [5] have studied experimentally the performance of Proof Of Work, Proof Of Stake, and also mixed methodologies. This study and other research are done in the performance evaluation of Proof of Stake and Proof of Work has ascertained that Proof Of Work Blockchain offers the highest reliability and fairness. However, Proof Of Work consumes the maximum amount of energy amongst the Blockchain methodologies.

a) Energy Consumption: Simple Proof Of Work systems reach the highest energy consumption levels and stay at those levels.
b) Fairness: Absolute proof of work models have the highest fairness where the coins are all distributed fairly and evenly across all nodes that are mining the coins. The coin age distribution is also quite even with pure proof of work.
c) Reliability of the System: Pure proof of work systems has excellent reliability in terms of performance and mining of coins or solving the equations that assures accurate block generation. The reliability also stays uniform throughout and doesn't vary much.

3. Proof Of Stake Performance

Based on results from Rong and Wai [5] studies, it is accepted that Proof Of Stake blockchain provides lower reliability and fairness when compared to Proof Of Work. However, Proof Of Stake consumes a lesser amount of energy when compared with Proof Of Work Blockchain methodology [6].

a) Energy Consumption: Pure Proof of Stake systems also do not have the least energy consumptions and this is rather in a mixed proof of stake and proof of work model. The energy consumption is also consistent at that energy level. Also, when Proof of Stake and Proof of Work is used in conjunction the energy levels are noticed to be lesser than that of pure proof of work – however, still quite high when compared to pure proof of stake blockchains except for a specific instance of mixed-mode.
b) Fairness: Pure proof of stake has the least fairness quotient and a large number of coins get distributed to the majority stakeholders. However, it is important to achieve proper analysis by mixing Proof of Stake and Proof of Work in the implementation with increased proof of work usage resulting in increased fairness that is equity in the distribution of the coins across all mining nodes.
c) Reliability of the System: Pure proof of stake has very little reliability from an assurance of generation of blocks and performance of the system. Pure proof of stake systems also has the reliability varying quite a bit over extended periods. Mixing proof of stake and proof of work, however, automatically improves the system's reliability and also provides continuity for the efficiency of the system.

4. Key Security Concerns Impacting Blockchain

a) Denial of Service (DoS) attacks require the attackers to flood the nodes and hence disrupt the normal functioning of the blockchain
b) Sybil attacks require the attackers to create misbehaving nodes (which can perpetuate fraudulent transactions) and hence disrupt the blockchain.
c) Mining has the attacker disclosing only those mined blocks that can result in the wastage of other equal miners who have to mine the extra blocks even though the attackers have already extracted. This expends the reasonable miners' computing resources.
d) Short range attacks, such as stakeholder bribing.
e) Long range attacks requires the attacker to start at the genesis block (first block) or some of the earliest blocks and create blocks to achieve a blockchain longer than the actual blockchain.
f) Coin age accumulation attack where coins are accumulated by the attacker and used fraudulently
g) Pre-computing attack in which the attacker has a list of all passwords stored in an easily accessible database across all blocks that can then be used to access any block inside the blockchain easily.

5. Proof Of Work Security Concerns and Solutions

*When compared to proof of stake implementation proof of work is relatively secure. However, even a well-written proof of work blockchain is susceptible to much vulnerability. The key vulnerabilities and their impact on Proof Of Work blockchain is listed in the table below.*TABLE 1*:* VULNERABILITIES OF PROOF OF WORK BLOCKCHAIN

Attack	**Is Proof Of Work Vulnerable?**
DoS	Yes
Selfish Mining	Yes
Short-Range Attack	No
Long-Range Attack	No
Coin-Age accumulation Attack	No
Pre-Computation Attack	No
Sybil Attack	Yes

6. Proof Of Stake Security Concerns and Solutions

In pure-play proof of stake implementations [3], security is a major concern. Where the total hash-rate of the device can estimate the susceptibility to attacks is proof of work, there is no equivalence in proof of involvement. Some of the major concerns in proof of stake implementations are,

a) Even distribution of stakes amongst users make it susceptible to forking attacks
b) Alternatively, if present users with very large stakes, they can interrupt the operations for example by promoting fraudulent operations

Delegated proof of stake is an extension of the proof of stake that extends the proof of stake and makes it more secure. In a delegated proof of stake, delegated miners mine the blocks and some of them need to sign the created blocks to make it valid. This to a large extent solves the vulnerabilities of the proof of stake mechanism [4].

*A contrast of stake proof and delegated stake proof against known attacks.*TABLE 2*:* VULNERABILITIES OF PROOF OF STAKE AND DELEGATED STAKE BLOCKCHAIN

Attack	**Is Proof Of Stake Vulnerable?**	**Is Delegated Proof Of Stake Vulnerable?**
DoS	Yes	Yes
Selfish Mining	No	No
Short-Range Attack	Yes	No
Long-Range Attack	Yes	Yes
Coin-Age accumulation Attack	Yes	No
Pre-Computation Attack	Yes	No
Sybil Attack	Yes	Yes

7. Conclusion

Pure play proof of work blockchain implementations have major issues of escalating energy consumption and have been proven as quite un-sustainable. Specifically, Bitcoin is a major example where it has been noted that the total energy consumed by all miners across the Bitcoin miner community would be greater than the per year energy consumption of some developed European countries. This makes pure proof of work systems an option that should be avoided if possible. However, pure proof of stake also has low and inconsistent reliability and low fairness issues that are major concerns. They also have substantial security vulnerabilities that would restrict their use to a very restricted private implementation and limit the adoption of these systems on a wide scale.

8. Future Scope of Work

Proof of Stake and Proof of Work implementation improves the consumption of energy, provides reliability and fairness. Using proof of work will also negate some key security vulnerabilities that will make the system sustainable, secure, and preformat. The researcher intends to pursue this path in creating a system that gets the most beneficial of both Proofs of Stake and Proof of Work worlds. The key here is to use it with suitable proportions. As a further step, the researcher will determine the correct algorithmic steps and the usage of Proof of Stake and Proof of Work across these steps in a blended manner to implement an industry usable application. The researcher also has multiple implementations lined up that will use the blended Blockchain methodology in a re-useable an adaptable manner.

REFERENCES

[1] Gervais A. On the Security and Performance of Proof of Work Blockchains. A. Gervais, G. O. Karame, K. Wüst and others. CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016.
[2] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System https://pdos.csail.mit.edu/6.824/papers/bitcoin.pdf
[3] Buterin V. Proof of stake: How I learned to love weak subjectivity. Vitalik Buterin. Ethereum Blog: https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity
[4] O. Vashchuk, R. Shuwar. Pros and cons of consensus algorithm proof of stake. Difference in the network safety in Proof of Stake and Proof of Work. 2018.
[5] Rong Zhang and Wai Kin (Victor) Chan. Evaluation of Energy Consumption in BlockChains with Proof of Stake and Proof of Work. 2020
[6] P.Rajitha Nair, Dr. Ramya Dorai , Vinod Unnikrishnan. Review of various Blockchain Based SSL Techniques. 2019 https://www.rsisinternational.org/journals/ijrsi/digital-library/volume-6-issue-5/74-76.pdf
[7] F. Imbault, M. Swiatek, R. de Beaufort, R. Plana 'The green blockchain Managing decentralized energy production and consumption', IEEE 2017
[8] PwC, 'Blockchain and smart contract automation: How smart contracts automate digital business', 2016
[9] Kamanashis Biswas, Vallipuram Muthukkumarasamy, 'Securing Smart Cities Using Blockchain Technology' 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems, 2016
[10] Konstantinos Christidis, Michael Devetsikiotis,'Blockchains and Smart Contracts for the Internet of Things' IEEE. VOLUME 4, 2016
[11] Chad Brubaker, Suman Jana, Baishakhi Ray, Sarfraz Khurshid,Vitaly Shmatikov 'Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations' 2014 IEEE Symposium on Security and Privacy
[12] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, 'Blockstack: A global naming and storage system secured by blockchains,' in USENIX Annual Technical Conference (ATC), June 2016
[13] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, 'SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies,' in IEEE Symposium on Security and Privacy (S&P), May 2015
[14] Feiyan Mu Jiafen Zhang and Jing Du, Jie Lin 'Application of the Secure Transport SSL Protocol in Network Communication' Fourth International Symposium on Computational Intelligence and Design, 2011
[15] Guy Zyskind, Oz Nathan, and Alex Pentland, 'Enigma: Decentralized Computation Platform with Guaranteed Privacy.' 2015