5. If the hash meets a certain difficulty level set by the network, the miner is allowed to broadcast the block to the network and claim the reward.

Proof of Authority is a blockchain algorithm that is designed for private blockchains. It is used in situations where the identities of participants are known and trusted. PoA is energy-efficient and provides faster transaction times. However, it is not suitable for public blockchains[5].

6. The miner must modify the nonce and continue the procedure until a valid hash is discovered if the hash does not satisfy the level of difficulty.

7. Other network nodes check the block's hash once it has been broadcast by a miner and then include it in their own copy of the blockchain.

3.2. Methodology of Proof of Stake

The Proof of Stake (PoS) approach involves set of guidelines and processes which decide how the consensus algorithm operates within a blockchain network[2]. Here are some key aspects of the PoS methodology:
Algorithms:-

1. Validator selection: Based on the amount of cryptocurrency they have staked, select a group of validators to create the next block. The probability of being selected as a validator is directly proportional to the amount of cryptocurrency staked.
2. Transaction verification: Each validator verifies the transactions that are added to the block, ensuring that they are valid and compliant with the network's rules.
3. Block creation: Once the transactions are verified, validators create a new block by adding the transactions to the blockchain.A challenging cryptographic method or problem must be solved in this procedure, which calls for a sizable amount of processing power.
4. Consensus: Validators must reach consensus on the validity of the transactions and the new block before it can be added to the blockchain.In order to maintain the network's security and defense against assaults, this procedure could include a voting system or other method.
5. Reward and penalty: Validators who successfully validate transactions and create new blocks are rewarded with cryptocurrency as an incentive to participate in the network. However, validators who act against the network's best interests or attempt to manipulate the consensus mechanism may face penalties or have their stake slashed.
6. Repeat: The process is repeated for each subsequent block, with validators being selected based on their staked cryptocurrency for each round.
7. The top N delegates (where N is a predefined number) with the most votes become block producers.
8. Block producers take turns producing blocks in a round-robin fashion.
9. Each block producer signs their produced block with their private key and broadcasts it to the network.
10. By confirming the digital signature and transaction history, other network nodes authenticate the block.
11. Once a block has been validated by a sufficient number of nodes, it is added to the blockchain.
12. The block producer is rewarded with transaction fees and newly created tokens.
13. Token holders can vote to remove a delegate from their position if they no longer trust them.

3.3. Methodology of Proof of Authority

Proof of Authority (PoA) is a consensus algorithm used in some blockchain networks to achieve consensus among network participants. In PoA, a set of pre-approved authorities or validators are responsible for creating and validating new blocks[1][26]
Algorithms:-

1. There are a number of previously approved authorities. These decision-makers are chosen in accordance with their standing, area of specialization, or relationship to the network.

2. The authorities take turns creating and validating new blocks. In a round-robin fashion, each authority takes turns creating and validating new blocks on the network.

3. Each block created is signed by the authority that created it. Each block created by an authority is signed with their private key to ensure its authenticity.

3.4. Methodology of Delegated Proof of Stake

Delegated Proof of Stake (DPoS) is a consensus algorithm used in blockchain networks to achieve consensus among network participants. In DPoS, token holders elect a set of validators or "delegates" to produce and validate new blocks[4].
Algorithms:-
1. Token holders stake their tokens to vote for delegates.
2. Delegates register their intent to become a block producer.
3. Token holders vote for their preferred delegates.

4. By confirming the digital signature and transaction history, other network nodes authenticate the block. By confirming the digital signature and transaction history, other network nodes authenticate the block.

5. Once a block has been validated by a sufficient number of nodes, it is added to the blockchain. Once a block has been validated by a sufficient

number of nodes, it is added to the blockchain, and the transaction history is updated.

6. Authorities are incentivized to act honestly through rewards or penalties. Authorities are incentivized to act honestly by receiving rewards for creating and validating blocks, or by facing penalties if they act maliciously.

7. A new authority can be added to the network if approved by the existing authorities. If a new authority is to be added to the network, they must be approved by the existing authorities.

8. A current authority can be removed from the network if they are found to be acting maliciously. If an existing authority is found to be acting maliciously, they can be removed from the network.

9. The network's nodes are incentivized to act honestly through rewards or penalties. Nodes receive rewards for taking part in the consensus protocol and enhancing network security. If nodes engage in malicious behavior, they risk punishment.

3.5. Methodology of Byzantine Fault Tolerance

BFT is a consensus algorithm for byzantine fault tolerance designed to enable a distributed system to reach agreement despite the presence of faulty or malicious nodes. BFT systems aim to achieve consistency and liveness in the presence of Byzantine faults, where nodes may fail in arbitrary and unpredictable ways[4].
Algorithms:-

1. A set of nodes is selected to participate in the consensus protocol. The number of nodes is typically predetermined to ensure the security and efficiency of the network.

2. Every node in the network sends a proposition to every other node. The proposal contains the proposed transaction that would be added to the blockchain as well as its sequence number.

3. Each node receives all proposals from all other nodes in the network.

4. Each node broadcasts its proposed decision to all other nodes in the network.

5. Each node receives all proposed decisions from all others in the network, nodes.

6. Each node gathers all proposed decisions and computes the final decision.

An algorithm for blockchain is called Federated Byzantine Agreement used in some blockchain networks to achieve consensus among a group of federated nodes. FBA is based on the idea of a quorum system, where a set of nodes (called a quorum slice) is required to agree on a decision for it to be accepted[5].
Algorithms:-

1. To take part in the consensus procedure, a set of nodes is chosen. Usually, these nodes are chosen based on their standing, knowledge, or involvement in the network.
2. Each node maintains a list of other nodes it trusts. These trusted nodes are part of the node's quorum slice.
3. Each node receives a proposal from another node in its quorum slice. The proposal includes the proposed transaction to be added to the blockchain and the sequence number of the proposal.
4. Each node sends its own proposal to all other nodes in its quorum slice.
5. Each node gathers all proposals from all other nodes in its quorum slice.
6. Each node computes the final decision based on a threshold of approvals. A suggestion is recognised as the final decision if a particular threshold of trustworthy nodes have approved it.
7. Each node broadcasts the final decision to all other nodes in the network.
8. Each node receives the final decision from all other nodes in the network.
9. The final decision is accepted if it is the same across all nodes in the network. The consensus technique is repeated until consensus is attained if the ultimate.

4. Experimental Model

Complete five tests using proof of work, proof of stake ,Delegated proof of stake, proof of authority, Byzantine fault tolerance, Federated Byzantine Agreement by comparing the number of blocks mined by each consensus algorithm. The test is carried out on a computer with an Intel Core i5-10210U CPU running at 1.60GHz and 2.11GHz with 8GB of AM. These algorithms were developed using Windows 10 with Intellij Idea 2020.3.1.

5. Evaluation Parameters

The consensus algorithm's performance is evaluated based on two factors:

A) the number of blocks mined.
B) the time taken to mine each block.

6. Experimental Result and Analysis

Table 1 and Table 2 list the first through fifth blocks, along with the times at which each block was mined using a particular consensus method, in five distinct ways.

Table 1. Time to mined block (1).

Mined Block Number of block	Time (ms)		
	Proof of work	Proof of stake	Delegated proof of stake
1	630	1064	641
2	1133	1411	1168
3	1435	515	1248
4	1324	1857	1690
5	2041	2264	3297

Table 2. Time to mined block (2).

Mined Block Number of block	Time (ms)		
	Proof of authority	Byzantine fault tolerance	Federated Byzantine Agreement
1	819	615	720
2	1633	1239	1170
3	1918	1556	1662
4	2128	1786	1700
5	2831	1566	1914

By analyzing the above data, it shows that the performance of different consensus algorithms varies depending on the number of blocks mined. Among the tested algorithms, Byzantine Fault Tolerance (BFT) and Federated Byzantine Agreement (FBA) consistently outperformed Proof of Authority (PoA), Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS) in terms of time taken to mine blocks. BFT had the lowest time taken in most cases, followed closely by FBA. PoW and PoS had comparatively higher times taken, and DPoS and PoA had the highest times taken. These findings suggest that BFT and FBA may be suitable for use in systems that require fast block times and high levels of security, while PoW and PoS may be better suited for systems that are less performance-sensitive and require more energy-efficient consensus algorithms.

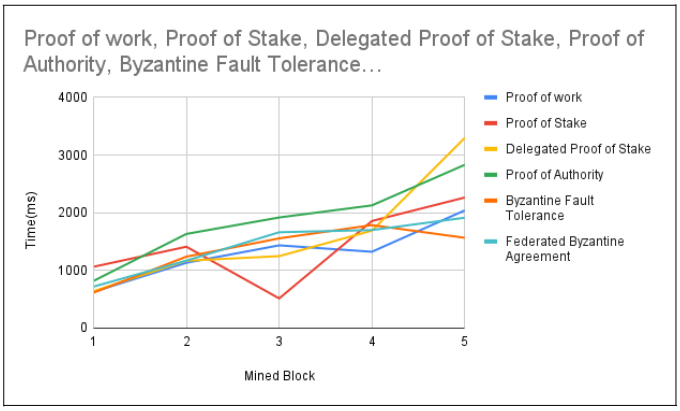

Figure 1. Mined Block vs Time

6. Conclusion

The results of our study show that each consensus algorithm has its own strengths and weaknesses. Proof of Work (PoW) is the most time-consuming and energy-intensive of the algorithms studied, while Delegated Proof of Stake (DPoS) and Proof of Stake (PoS) are faster and more consistent in their block mining times. However, DPoS requires a small set of trusted nodes, which may lead to centralization. Proof of Authority (PoA) is also fast and stable, but it requires a pre-approved list of validators, which may also lead to centralization.Federated Byzantine Agreement (FBA) and Byzantine Fault Tolerance (BFT) are designed to achieve fast finality, with FBA requiring a smaller set of nodes to operate efficiently. Ultimately, the choice of consensus algorithm depends on the specific needs of the network and its users.

7. Summary

The comprehensive analysis of blockchain algorithms aims to address specific research questions related to their performance, effectiveness, scalability, security, and trustworthiness. The selected algorithms represent widely used and prominent ones in the field, and the data for the analysis includes real-world implementations and theoretical data. Evaluation metrics are used to assess the algorithms, and their standardization and acceptance within the blockchain research community are considered. The analysis makes certain assumptions that may impact the generalizability of the findings.

Scalability and resource requirements are considered, and limitations and challenges encountered during the analysis are addressed to ensure accuracy and reliability. The analysis contributes new insights and advancements to the existing body of knowledge on blockchain algorithms. Comparative analysis is conducted, allowing for direct comparisons between different algorithms, and the findings provide key conclusions in this regard. Security and trustworthiness aspects, as well as potential vulnerabilities and attack vectors, are considered and evaluated. Ethical

considerations, particularly privacy and confidentiality, are taken into account during the analysis. Practical applications and recommendations are provided for practitioners and developers working with blockchain systems. Energy efficiency and environmental impact are considered, addressing the criticism of high energy consumption in blockchain technology. The strengths and weaknesses of the analysis impact the overall validity and reliability of the findings. The analysis contributes to the selection and design of blockchain algorithms for specific use cases and suggests implications for future research in the field.

References

[1] Panda S.K., Dash S.P., Jena A.K. (2021) Optimization of Block Query Response Using Evolutionary Algorithm. In: Bhateja V., Satapathy S.C., Travieso-González C.M., Aradhya V.N.M. (eds) Data Engineering and Intelligent Computing. Advances in Intelligent Systems and Computing, vol 1. Springer, Singapore. https://doi.org/10.1007/978-981-16-0171-2_54

[2] Nanda, S.K., Panda, S.K., Das, M., Satapathy, S.C. (2022). Automating Vehicle Insurance Process Using Smart Contract and Ethereum. In: Chakravarthy, V.V.S.S.S., Flores-Fuentes, W., Bhateja, V., Biswal, B. (eds) Advances in Micro-Electronics, Embedded Systems and IoT. Lecture Notes in Electrical Engineering, vol 838. Springer, Singapore. https://doi.org/10.1007/978-981-16-8550-7_23.

[3] Varaprasada Rao, K., Panda, S.K. (2023). Secure Electronic Voting (E-voting) System Based on Blockchain on Various Platforms. In: Satapathy, S.C., Lin, J.CW., Wee, L.K., Bhateja, V., Rajesh, T.M. (eds) Computer Communication, Networking and IoT. Lecture Notes in Networks and Systems, vol 459. Springer, Singapore. https://doi.org/10.1007/978-981-19-1976-3_18

[4] Varaprasada Rao, K., Panda, S.K. (2023). A Design Model of Copyright Protection System Based on Distributed Ledger Technology. In: Satapathy, S.C., Lin, J.CW., Wee, L.K., Bhateja, V., Rajesh, T.M. (eds) Computer Communication, Networking and IoT. Lecture Notes in Networks and Systems, vol 459. Springer, Singapore. https://doi.org/10.1007/978-981-19-1976-3_17

[5] Panda SK, Mohammad GB, Nandan Mohanty S, Sahoo S. Smart contract-based land registry system to reduce frauds and time delay. Security and Privacy. 2021; e172. https://doi.org/10.1002/spy2.172.[23] Panda, S.K., Satapathy, S.C. Drug traceability and transparency in medical supply chain using blockchain for easing the process and creating trust between stakeholders and consumers. Pers Ubiquit Comput (2021). https://doi.org/10.1007/s00779-021-01588-3

[6] Panda, S.K., Sathya, A.R., Das, S. (2023). Bitcoin: Beginning of the Cryptocurrency Era. In: Panda, S.K., Mishra, V., Dash, S.P., Pani, A.K. (eds) Recent Advances in Blockchain Technology. Intelligent Systems Reference Library, vol 237. Springer, Cham. https://doi.org/10.1007/978-3-031-22835-3_2

[7] Murala, D.K., Panda, S.K., Sahoo, S.K. (2023). Securing Electronic Health Record System in Cloud Environment Using Blockchain Technology. In: Panda, S.K., Mishra, V., Dash, S.P., Pani, A.K. (eds) Recent Advances in Blockchain Technology. Intelligent Systems Reference Library, vol 237. Springer, Cham. https://doi.org/10.1007/978-3-031-22835-3_4

[8] Rao, K.V., Murala, D.K., Panda, S.K. (2023). Blockchain: A Study of New Business Model. In: Panda, S.K., Mishra, V., Dash, S.P., Pani, A.K. (eds) Recent Advances in Blockchain Technology. Intelligent Systems Reference Library, vol237. Springer, Cham. https://doi.org/10.1007/978-3-031-22835-3_9

[9] Nanda, S.K., Panda, S.K., Das, M., Satapathy, S.C. (2023). Decentralization of Car Insurance System Using Machine Learning and Distributed Ledger Technology. In: Bhateja, V., Yang, XS., Chun-Wei Lin, J., Das, R. (eds) Intelligent Data Engineering and Analytics. FICTA 2022. Smart Innovation, Systems and Technologies, vol 327.Springer, Singapore. https://doi.org/10.1007/978-981-19-7524-0_52

[10] Agarwal N., Jain A., Gupta A., Tayal D.K. (2022) Applying XGBoost Machine Learning Model to Succor Astronomers Detect Exoplanets in Distant Galaxies. In: Dev A., Agrawal S.S., Sharma A. (eds) Artificial Intelligence and Speech Technology. AIST 2021. Communications in Computer and Information Science, vol 1546. Springer, Cham. https://doi.org/10.1007/978-3-030-95711-7_33.

[11] Agarwal, N., Srivastava, R., Srivastava, P., Sandhu, J., Singh, Pratap P. Multiclass Classification of Different Glass Types using Random Forest Classifier. 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022. p. 1682-1689.

[12] Agarwal, N., Singh, V., Singh, P. Semi-Supervised Learning with GANs for Melanoma Detection. 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022. p. 141-147.

[13] Tayal, D.K., Agarwal, N., Jha, A., Deepakshi, Abrol, V. To Predict the Fire Outbreak in Australia using Historical Database. 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2022. p. 1-7.

[14] Agarwal, N., Tayal, D.K. FFT based ensembled model to predict ranks of higher educational institutions. Multimed Tools Appl 81, 2022.

[15] Ghosh, H., Tusher, M.A., Rahat, I.S., Khasim, S., Mohanty, S.N. (2023). Water Quality Assessment Through Predictive Machine Learning. In: Intelligent Computing and Networking. IC-ICN 2023. Lecture Notes in Networks and Systems, vol 699. Springer, Singapore. https://doi.org/10.1007/978-981-99-3177-4_6

[16] Alenezi, F.; Armghan, A.; Mohanty, S.N.; Jhaveri, R.H.; Tiwari, P. Block-Greedy and CNN Based Underwater Image Dehazing for Novel Depth Estimation and Optimal Ambient Light. Water 2021, 13, 3470. https://doi.org/10.3390/w13233470

[17] G. P. Rout and S. N. Mohanty, "A Hybrid Approach for Network Intrusion Detection," 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 2015, pp. 614-617, doi: 10.1109/CSNT.2015.76.