A Deep Dive into Blockchain Consensus Protocols

***Abstract*— Blockchain is the backbone of digital cryptocurrency systems, and it eliminates the need for a central authority in a decentralized network. Blockchain is a system that allows the sharing of information securely and transparently in a peer-to-peer connected decentralized network consisting of untrustable users. Blockchain technology ensures security, equality, and fairness of the system by following a well-defined set of rules known as a consensus protocol. These consensus protocols are at the core of blockchain technology and secure the network from various attacks and frauds. It is nearly impossible to breach a system following these protocols. There are various consensus protocols, each with its advantages and disadvantages. In this paper, we have discussed various consensus protocols in terms of performance, fairness, resource requirements, and security breaches. We have discussed the working of typical blockchain technology by describing major concepts in the implementation of bitcoin technology. We also discussed the most common security breaches in decentralized systems.**

Keywords*— *Blockchain, distributed consensus protocol, Permissionless Blockchain, Permissioned Blockchain

I. INTRODUCTION

A blockchain is a system of entities connected in a peer-to-peer distributed network. It was implemented in the year 2008 and 2009 by a person or a group of people under the pseudonym of Satoshi Nakamoto. [1] The earliest application of blockchain technology was to transform the way traditional transaction management systems work. A conventional transaction management system relies on a central authority to provide functionality and security to the system. Over time many concerns of privacy, efficiency, and security have been raised in the context of traditional systems. Blockchain aims to eradicate the need of central authorities and proposes a decentralized system that attempts to solve all the above-mentioned problems of traditional systems. Blockchain offers a platform for entities that do not trust each other to work and share information in the network reliably and securely. In the blockchain, we study the algorithms and ideas that make such a system consisting of untrustable entities reliable and secure. Bitcoin is the first application of blockchain technology that allows its users to send digital currency, also known as bitcoin, across the network anonymously and without any charges. Blockchain is not restricted to the financial sector only, and it is being adopted in other fields like education, government, healthcare and etc. Another application of blockchain technology is implementing Dapps, which use smart contracts (automated programs working on a blockchain) and blockchain as the backend to achieve decentralization. [2] Blockchain Technology has five crucial characteristics: Decentralization, Persistence, Privacy, Transparency, and Integrity. Decentralization and Transparency are the core working principle which evades the need for centralized transactions. Persistence and Integrity can be attributed to the forefront principle, which disallows any kind of data deletion or modification of existing blocks. This technology also has protocols to ensure the privacy of sensitive information to some level. In this paper, we have discussed blockchain technology in detail, how it achieves decentralization, security, consensus, and anonymity, and some of the common problems seen while building a good blockchain consensus protocol. As blockchain is being used for more than just financial sector applications, some consensus algorithms are better suited for particular applications. We have discussed various consensus protocols with their advantages and disadvantages. The paper is organized in four sections. Section 2 explains blockchain technology and common problems related to it. In section 3, we describe various popular consensus algorithms, and section 4 presents the conclusion.

II. BLOCKCHAIN TECHNOLOGY

This section discusses working and some of the implementation details of the most popular blockchain technology, bitcoin. Bitcoin network is a peer-to-peer network meaning all nodes are equal, and each node provides and consumes network services. Bitcoin uses the elliptic curve multiplication functions at its core. These functions are irreversible, meaning easy to calculate in one direction but impractical to compute in the opposite direction. In the bitcoin network, a user is identified by its private key. All private keys are unique. A user can have multiple private keys. A private key is a secret key that controls bitcoin access, and the one having this key is supposed to be the owner of the bitcoin. Because the private key cannot be shared with anyone else, a public key is derived from the private key by applying the elliptic curve multiplication on the private key and the generator point. [1]

Public key = Private Key * Generator Point.

This cryptographic function allows calculation of the public key from the private key, but the reverse is practically impossible. The knowledge of public key doesn't give bitcoin access but uniquely identifies a user and can be distributed publicly to receive funds. A further abstraction level over the public key is a bitcoin address, a more human-readable form of the public key. Still, it doesn't give bitcoin access, and it is derived from the public key using a one-way cryptographic function. [1]

The private key is generated randomly from a vast space of available private keys. Private keys are 256 bits long and can lie between 1 and n-1, where n is a constant slightly less than 2^256, also known as the elliptic curve's order. A private key is generated by feeding in a large random string to the SHA256 (Secure Hash Algorithm) algorithm that produces a 256-bit long hash value, which can be used as the private key provided it lies between 1 and n-1. [1]

Another important concept that blockchain technology uses is digital signatures. A digital signature is similar to the conventional handwritten signature, and a valid digital signature ensures a valid transaction of funds on the bitcoin network. A digital signature scheme consists of two parts: First, an algorithm to compute a signature, provided a private key and a message, and second, the validity of the signature is easily verifiable by anyone who knows the message, and the public key corresponding to the private key used to generate the signature. [1]

Therefore, a valid signature also ensures the absence of any malicious modifications in the message. The signature algorithm also incorporates a random factor in the calculation so that every time a different signature is generated, even if the same message and private key are provided. [1]

The bitcoin owner digitally signs each transaction, and any node in the network can verify the ownership of the bitcoin by verifying the signature on the transactions. A transaction in the bitcoin network contains transaction inputs and transaction outputs. Transaction inputs consist of unspent bitcoins possessed by the private key, and transaction outputs consist of the desired change of ownership of bitcoin. It is common to include transaction fees in the transaction itself. In such cases, the sum of bitcoin values in output is lesser than the sum of bitcoin values in input, and the difference is given to the miner as a reward. There are various schemes to calculate transaction fees, such as fixed transaction fees, based on the size of the transaction in KB, based on the transaction's value, etc. Including transaction fees in the transactions ensures the system's security by making it economically infeasible for an attacker to flood the network with transactions. [1] The transactions are grouped into blocks, and a block is a data structure to store transactions that use Merkle trees to query the transactions stored in it efficiently. Each block contains nearly 500 transactions and links back to the previous block, known as the parent block, forming a linked list of blocks known as the blockchain. The linking of a block to the previous block restricts modification of transactions in the blockchain as a modification in any transaction changes the hash value of the block containing transaction and forcing the recomputation of all subsequent blocks, thus making the blockchain immutable. The blocks are created by miners to add the next block in the chain. [1]

A miner is a node that validates transactions coming into the network, forms a block containing the transactions, and competes with other miners to solve a cryptographically hard problem to add its block to the blockchain and obtain the newly mined bitcoin currency as its reward. The mining process incentivizes the miners to validate the transactions and ensures the decentralized security of the network by aligning the actions of participants in the direction of network security. [1]

Mainly, there are two kinds of blockchain categories. They are permissionless blockchain and permissioned blockchain. The permissionless blockchain, also known as the public blockchain and permissioned blockchain, is further classified into the consortium and fully private blockchain. A public blockchain is an open blockchain accessible to everyone. All nodes have equal power to validate transactions and participate in the mining process. There is no presence of any centralized authority. Bitcoin technology comes under the public blockchain. [1] [3]

A consortium blockchain, also known as a semi-decentralized blockchain, consists of a few nodes having the privilege to validate transactions and make decisions. In contrast, all other nodes can validate transactions and make decisions only after achieving a consensus. [3] [1]

A fully private blockchain consists of a central authority having all the privileges to validate transactions and make decisions. Permissioned blockchains are easier to maintain and implement than permissionless blockchains. [1] [3]

There are many problems that an exemplary implementation of blockchain technology aims to solve. Some of those problems are described below.

Sybil Attack: It is an attack in which a user creates many identities and tries to gain a disproportionately large influence on the network and thereby execute its malicious activities. Different identities appear to act independently of each other to the system but are controlled by the malicious user. A system's vulnerability to a Sybil attack depends on the cost of generating identities in the system and the degree to which the system accepts input from an untrusted identity. [4]

Double Spending Attack: It is the risk that a malicious user can spend a digital currency more than once by creating illegitimate multiple copies of the currency. A system's vulnerability to a double-spending attack depends on the difficulty and cost of making copies of digital currency and the difficulty of verifying a digital currency's legitimacy. [1] [4]

Byzantine Generals' Problem: The risk of a system not being able to form a consensus among participating nodes, which is critical to the system's operation due to malicious activities performed by some of the nodes in the system. [5]

Collusion Attack: An attack in which a node establishes a secret agreement with an adversary to perform malicious activities in the system. [4]

Denial of Service Attack: An attack to flood the system with huge traffic making the system inaccessible to intended users. [4]

III. Consensus algorithms

Consensus protocol in blockchain technology is a set of rules accepted and used by all the nodes in the system to form a conclusive consensus regarding the addition and legitimacy of a new block to be added in the chain. The consensus protocols are designed in a way to tackle and mitigate the risk of most of the known attacks and to increase the efficiency and decrease the resource requirements of the system. One consensus protocol is not suitable for all the applications. Therefore, a substantial amount of work has been done by researchers to design many protocols, some of which we have discussed in this section.

A. Proof of Work

The first and most widely used Consensus Protocol used in blockchain to reach consensus is Proof of Work (PoW). It involves miners to participate in a competition to solve a mathematical puzzle that is based on costly computer computation involving Hashing (SHA-256), Merkle Tree, and P2P networks for all operations on the blocks created in the blockchain [6]. The puzzle is generally not relevant; it is to make sure the miners dedicate computation power as an investment to prove they are not malicious. A miner who solves the puzzle first is rewarded accordingly. The person who finally adds the block to the chain receives coins as a reward for their work, and as soon as a miner solves the puzzle and the block is added to the blockchain, the transaction is considered to be complete. After the victory, the miner broadcasts the block over the network, and it is verified by others. In case of any conflicts, the multiple

branches in the chain are extended, but only the longest chain prevails [6]. The miner with x fraction of total computation power has x probability of getting the reward to make it fair for every participant.

The requirement of substantial computation power and difficulty level makes it nearly impossible for solo miners to solve the puzzle. This is regarded as a waste of resources due to significant computational power put into doing no useful work. The requirement of high computational power ensures high security as the malicious user requires 51% of computation power to perform a potential attack [7]. Specific expensive hardware like Application-Specific Integrated Circuit (ASIC) makes the mining process unfair by giving some miners an unfair advantage.

B. Proof of Stake

Proof of Stake provides a solution to the substantial computational requirement of PoW. In PoS, the miners aren't required to solve a puzzle; instead, the miner with the highest stake will get a chance to add a block to the chain [8]. This response to the challenge of computation is called Minting [9] [3]. Although this protocol is based on an economic stake, but having a maximum stake doesn't ensure a miner with the highest stake will necessarily be selected [3]. Similar to a lottery, the validator is chosen by the system randomly. The higher the stakes of the miner, the higher are the chances of the miner to add the next block, i.e., if a miner holds a 35% stake in blockchain, then that participant has a 35% chance of mining the next block. As no coins are being generated in this protocol, there is no reward for miners other than transaction fees.

As the one with a higher stake has a higher chance to mine the next block, it benefits the rich and widens the gap with the poor even more [3]. After some time, finally, a person of a group may own more than 50% of the chain, threatening the decentralization. To avoid this, there are economic punishments designed to punish conspiring parties. Now since the major stakeholder is the only one who can decentralize the chain, they will avoid doing so in fear of losing the stake.

C. Delegated Proof of Stake

Delegated Proof of Stake (DPoS) is the most common variant of Proof of Stake, which resembles indirect democracy. In DPoS, instead of validating the block themselves, stakeholders elect validators/delegates. 21-100 validators are selected, and they keep changing according to an order to deliver blocks [7] [5]. This delegate, instead of competing with each other, join hands to create the block. [10] If a delegate makes a mistake or performs a malicious act, other delegates vote him out. It favors decentralization as it ensures stakeholders will choose those delegates who would give back better rewards [5]. They verify the honest intent of the delegate they vote for as their stakes are invested in them. This protocol is fast and efficient, solves the problem of double-spending, but the 51% attack is still a downside.

D. Leased Proof of Stake

Leased Proof of Stake (LPoS) is a less commonly used variant of PoS. It favors rich people to become more prosperous [3]. Node with the highest stake has the highest chance of creating a block in the Blockchain. It motivates the leasing participants for their aspiration of rewards, which are distributed equally among the validators as per their stake in Blockchain.

E. Proof of Elapsed Time

Proof of Elapsed time (PoET) is an efficient and fairest method used in the blockchain network, which was proposed by intel. It is similar to PoW but is more efficient as it requires less energy. It leverages the use of Trusted Execution Environments (TEE) [3]. Like PoW, in this protocol, miners need to solve a hash calculation problem, but there is no competition as there was in PoW. The winner is selected in a fair lottery system to improve the efficiency of the process. New miners must identify themselves before the algorithm introduce them to chains login and hence ensures security. In PoET, every miner has to wait for an assigned waiting time for block construction, which is monitored by protocol [7] [11]. The miner whose waiting time finishes first is victorious and then creates and broadcasts the block on the network. To ensure fairness, this protocol use Intel's Software Guard Extension (SGX) on which code for the whole process relies, and this SGX is available on most Intel CPUs. PoET does not disclose the identity of participants and maintains anonymity while reaching consensus. The drawback of PoET is its dependence on the TEE enabled hardware. This hardware ensures security from malicious programmers by not allowing more than one instance of the chain running on 1 CPU, so the participants do not create more than one instance to increase their chance of winning.

F. Proof of Burn

In the Proof of Work consensus protocol, all the miners compete to solve a cryptographically hard problem, and the successful miner gets to add the new block and gets rewarded. In this process, a lot of computational power and energy is lost, which could otherwise be used for useful work. Proof of Burn consensus protocol aims to solve this problem of resource wastage by using the strategy of burning the cryptocurrency coins to participate in the mining process. All miners send some amount of cryptocurrency coins to a verifiable un-spendable address and gain the right to create the next block in proportion to the coins burnt by them [12]. Depending on the implementation of the PoB, miners may be allowed to burn the native cryptocurrency or the cryptocurrency of different blockchains.

To mitigate the unequal distribution of mining power among participating nodes over time, PoB uses the concept of periodic burning of cryptocurrency. The value of burnt coins reduces as new blocks in the blockchain are added [12] [7]. It maintains consistent activity by miners and consistent equipment up-gradation to compete in the system and, therefore, strengthening the infrastructure of the blockchain. Slimcoin is an example of blockchain technology that implements the PoB consensus protocol.

G. Proof of Capacity

Proof of Capacity addresses the wastage of resources problem in PoW and uses hard disk space instead of computational power to provide security to the system [13]. This protocol works in two phases: Plotting and Mining [14].

The plotting phase consists of generating as many as possible random solutions to the mining puzzle that fits the hard disk

space dedicated to plotting and stores those solutions in a plot file. Plotting uses Shabal hashes, which are hard to compute and therefore are precomputed and stored [15].
The greater the size of space dedicated to plotting, the larger is the number of solutions generated and, therefore, increasing the probability of finding the solution and getting rewarded.
The mining phase consists of reading the solutions from the plot file and finding a solution that solves the problem. The miner who reaches the solution in the shortest time gets rewarded and adds the block in the blockchain.
The mining process only requires computational power for a few seconds to read the plot file and therefore is more energy-efficient than PoW [15] [14] [7].
Burstcoin and SpaceMint are two examples of blockchain technology that implements Proof of Capacity consensus protocol.

H. Proof of Activity

Proof of Activity combines the best of PoW and PoS. It works in two phases. The first phase uses PoW for the creation of a new block, in which all the miners compete to solve the cryptographically hard problem and create a block containing only the header and the address of the miner who mined the block and no transaction [16].
The second phase uses PoS to select some nodes at random as validators [16]. The work of these validators is to sign the block. A block is only added in the blockchain if it is signed by all the validators and therefore, ensuring miners to reach a consensus. A node having a higher stake in the system has a greater probability of being selected as a validator. If a block is not signed by all the miners, the process is moved to the next winning block.

I. Proof of Sincerity

Proof of Sincerity (PoSincerity) aims to solve the unfair distribution of the reward problem (a node with more computing power is more likely to get rewarded. It has a greater probability of solving the cryptographic puzzle while the node with low computing power stands nearly no chance to get rewarded) in Proof of Work.
Proof of Sincerity consensus algorithm introduces the concept of the sincerity of a node in a system; it is a measure of how sincere a node is to consume its resources to mine the next block in the chain. To mine a block, a miner has to find the solution of a cryptographically hard problem through randomly searching in the solution space and trying if the proposed solution is indeed a solution to the problem. This process of finding the solution requires the computation of hash codes with some number of leading zeros. One unit of the level of sincerity is a measure of a node to consume its resources for computing a hash code with one leading zero. Similarly, the definition extends for n units. [17] All the nodes participating in the mining process and having a certain sincerity level or above are rewarded irrespective of the node, which solves the cryptographic puzzle and adds the next block of transactions to the blockchain. A block of transactions is mined as long as there is at least one node having the necessary level of sincerity in the network to mine the block. All the nodes participating in the mining process and having the necessary level of sincerity are rewarded with respect to the ratio of their level of sincerity to the level of sincerity of the node, which successfully solves the cryptographic problem.

In table 1, we have summarized advantages and disadvantages of consensus protocols with blockchain platforms.

TABLE I.

S. No.	Consensus Protocol	Platform	Advantages	Disadvantages
1.	Proof-of-Work	Bitcoin, Ethereum	-Secure -highly scalable	-Energy intensive -vulnerable to 51% attack
2.	Proof-of-Stake	Ethereum, BITTO	-Higher speed -Lesser energy consumption -No specialized hardware requirement	-Richer gets richer and poor gets poorer. -vulnerable to 51% attack
3.	Delegated Proof-of-Stake	DDKoin,	-Better rewards distribution -secure real-time voting	-power is in the hands of a few, hence, more centralized
4.	Leased Proof-of-Stake	Waves	-Better distribution of rewards -Higher processing speed	-Cartel formations
5.	Proof-of-Elapsed Time	Hyperledger Sawtooth	-Low resource consumption -Better security	-Reliance on Intel's SGX (Software Guard Extension)
6.	Proof-of-Burn	Slimcoin	-Promotes regular activity -Resource efficient than PoW	-Wastes resources in the form of burnt coins -Vulnerable to 51% attack
7.	Proof-of-Capacity	SpaceMint, Burstcoin	-High energy efficiency -No requireme	-Redundant hard drive space

			nt of specialized hardware	-Prone to malicious softwares
8.	Proof-of-Activity	Decred	-Reduced probability of 51% attack.	-High energy consumption -Rich gets richer syndrome
9.	Proof-of-Sincerity	-	-Better reward distribution -Can be configured to prevent 51% attack	-More energy required than PoS

IV. Conclusion

Blockchain technology is secure, transparent, eliminates the need for centralized authority, and achieves consensus in a decentralized system. However, its advantages come at the cost of high computation power requirement, lack of scalability and lack of performance. This paper discussed the technical working of a typical blockchain network by describing some essential implementation details, most common attacks studied concerning the blockchain technology and thoroughly compared various popular consensus protocols being used in the industry. It also presents a concise comparison of all the mentioned consensus protocols, their advantages, disadvantages, platforms using those consensus protocols and the area where each protocol lacks in a tabular form.

A thorough comparison of various consensus protocols in this paper makes it quite evident that a single consensus protocol is not suitable for every use case. Therefore, many use cases targeted consensus protocols are developed. Further, blockchain technology can potentially revolutionize various sectors dependent on a central authority and make the system more transparent and secure.

References

[1] A. M. Antonopoulos, Mastering Bitcoin: unlocking digital cryptocurrencies, O'Reilly Media, Inc., 2014.

[2] P. Anand and A. Chauhan, "The Advent of Ownerless Businesses: Decentralised Autonomous Organisations," *International Journal of Scientific and Technology Research*, pp. 2848-2852, 2020.

[3] A. Wahab and W. Memood, "Survey of Consensus Protocols," in *arXiv preprint arXiv:1810.03357*, 2018.

[4] D. Dasgupta, J. Shrein and K. Gupta, "A survey of blockchain from security perspective," *Journal of Banking and Financial Technology*, pp. 1-17, 2019.

[5] L. Bach, B. Mihaljevic and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2018.

[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[7] K. Sharma and D. Jain, "Consensus Algorithms in Blockchain Technology: A Survey," in *10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2019.

[8] QuantumMechanic, "Proof of stake instead of proof of work," 11 July 2011. [Online]. Available: https://bitcointalk.org/index.php?topic=27787.msg349645#msg349645. [Accessed 5 January 2021].

[9] P. Hooda, "Proof of Stake (PoS) in Blockchain," 11 December 2019. [Online]. Available: https://www.geeksforgeeks.org/proof-of-stake-pos-in-blockchain/. [Accessed 5 January 2021].

[10] A. Chauhan, O. P. Malviya, M. Verma and S. T. Mor, "Blockchain and Scalability," in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion*, 2018.

[11] B. Curran, "What is Proof of Elapsed Time Consensus? (PoET) Complete Beginner's Guide," 11 September 2018. [Online]. Available: https://blockonomi.com/proof-of-elapsed-time-consensus/. [Accessed 5 January 2021].

[12] K. Karantias, A. Kiayias and D. Zindros, "Proof-of-burn," in *International Conference on Financial Cryptography and Data Security*, 2020.

[13] S. Dziembowski, F. Sebastian, K. Vladimir and P. Krzysztof, "Proofs of space," in *Annual Cryptology Conference*, Heidelberg, 2015.

[14] A. Hayes, "Proof of Capacity (Cryptocurrency)," 24 September 2020. [Online]. Available: https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp#:~:text=Proof%20of%20capacity%20(PoC)%20is,mining%20rights%20and%20validate%20transactions.. [Accessed 5 January 2021].

[15] P. Andrew, "What is Proof of Capacity? An Eco-Friendly Mining Solution," 31 January 2018. [Online]. Available: https://coincentral.com/what-is-proof-of-capacity/. [Accessed 5 January 2021].

[16] I. Bentov, C. Lee, A. Mizrahi and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]," in *ACM SIGMETRICS Performance Evaluation Review 42(3)*, 2014.

[17] Zaman, U. Miraz, S. Tong and M. Manki, "Proof of sincerity: A new lightweight consensus approach for mobile blockchains," in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2019.