Comparative Study on Consensus Protocols in a Decentralized Autonomous Network

Shanu Kumar
Dept. of Computer Science
CMR Institute of Technology
Bengaluru, India
shku19cs@cmrit.ac.in

Shraddha Sahay
Dept. of Computer Science
CMR Institute of Technology
Bengaluru, India
shsa19cs@cmrit.ac.in

Dr. M Raja
Dept. of Computer Science
CMR Institute of Technology
Bengaluru, India
raja.m@cmrit.ac.in

***Abstract*— Web3.0 is the next biggest revolution in the world of information technology in our age. Building trust-based systems based on blockchain technology leveraging the benefits of cryptography and decentralization in industries spanning across finance, retail, provenance and many more is the first step in exploring this technology. This paper aims to explore the functional characteristics of blockchain and compare various consensus mechanisms as the building blocks of such networks suited for specific DAOs.**

Keywords— Consensus Protocols, Blockchain, Decentralization, Consensus Mechanisms , DAO

I. INTRODUCTION

The blockchain industry has revolutionized the internet. Major shortcomings of internet, such as middlemen have been eliminated by a transparent, cryptographic trust-based system. The concept of a distributed peer to peer network was not a new concept in the industry, but the drawbacks of double spending and fraudulent transactions made it less efficient to use. The first ever framework for a peer-to-peer distributed system was introduced by Satoshi Nakamoto in his whitepaper [1]. It threaded together concepts of hash functions, digital signatures and public ledgers for a robust decentralized and distributed network.

With the introduction of smart contracts [2], the framework could now work as an automated system, giving birth to decentralized autonomous corporations [3] soon after the bitcoin paper in the 2008's. It was in 2013 that the term was widely accepted. They were described as a corporate governance, with shareholders holding tokens for the network. It was stated to be an incorruptible system with minimum human interference and publicly auditable.

The corporation term started getting linked to governance and later was widely accepted as decentralized autonomous organization(DAOs) in 2014. The first ever recognized DAO was "The DAO" [4] built over the Ethereum main-net as a hedge fund. This application resided on the fundamentals of "code is law" , but later due to a bug in the source code had the funds stolen, which lead to the legality controversy of the DAO's[5]. So, in today's world where there are ample applications of blockchain and blockchain hosted organizations, the legal nature of the DAOs can still be questioned.

The major workforce behind any distributed networks have an underlying blockchain framework. The essential components of a blockchain are the nodes, ledgers, consensus mechanisms and the block added on the chain. They are discussed in the components section.

The objective of this review is to discuss the various consensus protocols in a decentralized system. This paper presents a comparative analysis on the various consensus mechanisms available in a decentralized system and their use cases.

II. LITERATURE SURVEY

A consensus protocol as a system that ensures all nodes in the network agree on a given transactional history [6]. The earliest protocol to be exploited was the Proof of Work that laid down rewards for the winner node in the cryptographic puzzle solving race.

The excessive loss in computational resources in the network urged the blockchain to progress towards a better protocol called Proof of Stake, that calculated the weight of node as being proportional to its current currency holdings and not just computational powers [7].

The paper discusses in depth the history and development of consensus mechanisms in a permissionless network [8]. It takes an in-depth tour of state-of-the-art consensus protocol in permissionless consensus through zero knowledge proofs to a variety of proof of concept schemes proposed under the Nakamoto protocol, which are also listed in Table 1.

The major problem in designing the protocols were to manage the Byzantine fault tolerance of the network. This was solved through the YAC algorithm[9] , it guaranteed the liveness of the system, security and convergence of data stored in the ledgers.

Each application in the real world came with its own set of problems to be solved. The diversity of the applications lead to evolution of mechanisms. A larger set of protocols were custom made for each genre of usability. The paper [10] describes the protocols in major DAO platforms such as Moloch DAO, Aragon and DAO Stack.

A comparative study of most widely used protocols has been done under Section IV , Table 1.

III. COMPONENTS OF BLOCKCHAIN

A. Peer Nodes

Blockchain network consists of multiple computer systems called as nodes. Each node can be part of multiple channels and host their own local copies of the ledger to validate transactions on the network. The peer nodes are responsible for submitting, validating transactions, consolidating into blocks and adding these blocks to the chain.

B. Ledgers

Ledger is a key concept of blockchain that stores current values of the attributes for business object and the set of transactions which resulted in the current values. At any point in time the ledger can be queried to fetch both current

state as well as history of transactions, making the ledger a key tool to achieve immutability and transparency in a blockchain network. A ledger consists of two distinct, though related, parts – a world state and a blockchain. [11]

C. Blocks

Blockchain is a sequence of interlinked blocks. Each block contains a sequence of transactions, where transaction can be any query or update to the real-world state. The block in a DAO contains rule enforcement operation and financial transactions. The block contains mainly of cryptographic hash of previous block, a timestamp and transaction data in the form of Merkle tree. A transaction becomes a block only when verified and validated by the miners. Miners are the nodes that race to finish a computational puzzle and expend sufficient amount of their computing resources to validate the transaction and push the block on the chain. This act helps them earn tokens in the network.

D. Consensus Mechanisms

Consensus mechanism refers to the entire stack of protocols, actions and incentives that allow the network peers to agree on the state of the blockchain. The miner who wins the race in solving the computational problem gains an incentive while the other peers verify the new block using a consensus algorithm. The consensus algorithm is a technique that assists the network to reach an agreement [12].

The figure.1 demonstrates the various components of the blockchain network. The nodes are interconnected in a peer to peer distributed network. The network nodes interact with each other in terms of transactions. These transactions take place with the approval of the entire network through consensus protocols. Each transaction on verification and validation by the peers is then added to the blockchain as a valid block.

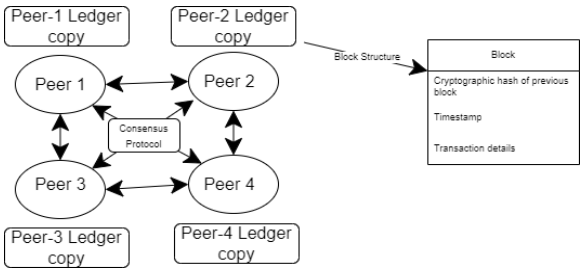

Figure.1 Components of the Blockchain

IV. CONSENSUS PROTOCOLS

A. CHARACTERISTICS

Blockchain is a conglomeration of all methodologies to overcome the drawbacks of the internet. It brings in the concept of trust by elimination of intermediate parties, along with a distinct framework for a distributed architecture that stands robust. Any blockchain system has following fundamental characteristics:

1.Transactions and Smart Contracts

A transaction is a data structure that encodes the exchange of assets between multiple parties in accordance to pre-established rules or contracts on a blockchain network. A smart contract is a set functions and rules that are executed during any transaction on the blockchain. They help in automatic rule enforcement in the chain.

2.Consensus and Trust

The nature of blockchain is such that there are no middlemen. This implies that there is no need for entities to trust each other. The network establishes trust based on group consensus enforced by validating transactions that comply to pre-determined smart contracts. Blockchain relies heavily on cryptographic hash functions and digital certificates to establish trust on each transaction. Hashing of each block ensures that the chain is immutable and presents a true image of the record of transactions at every instant.

3.Public and Private Blockchain

Blockchains can be classified as public, private or hybrid variants, depending on their application . Public blockchains are permissionless blockchains where anyone can join and participate. This negatively impacts the secrecy of the chain as any user can view the transaction amount and addresses. Private blockchains are permissioned networks, where only allowed participants can view and operate on the blockchain.

B. CONSENSUS MECHANISMS

Consensus algorithms are algorithms through which all the peers of a blockchain network reach a common acceptance or consensus about real time state of the distributed leger and basically used to achieve agreement, trust and security across a decentralized network. It sets rules that decide on the conformity of contribution made by various participants of the network. There are various consensus algorithms which are widely used out of which two of the most common or prevalently used mechanism are: Proof of Work and Proof of Stake. Proof of Elapsed is also a widely accepted protocol that provides equal fighting chance for every node. The latest applications are each using a modified version of the discussed protocols with parameters such as voting period, voting delay and queue time varying.

PROTOCOLS	FEATURES	DRAWBACKS
Proof of Work	This mechanism requires for the node to generate the proof for solving a cryptographic problem to be the first one to mine the transaction block. If the node is able to achieve it, it pushes the block onto the chain and gains incentives.	It drains a lot of computation resources of the network and needs a longer processing time.
Proof of Stake	This mechanism evolved as a low-cost, low-energy consuming protocol compared	It lead to the process of token hoarding more that spending.

	to PoW. It allows for maintaining the ledger by a participating node based on the amount of network token it currently holds. For each mining process, if tokens once staked cannot be staked for another transaction again, unless they are earned back.	
Proof of Burn	Proof of Burn has the user send their tokens to an unspendable address, in a way of burning them. The more coins a user invests the higher the chances to mine the next block.	The short term loss may again revert the users towards hoarding of coins for future needs.
Holographic Consensus	This mechanism resolves the scaling problem of the DAO. It allows for the quorum required for a proposal to be reduced from absolute majority to relative majority. The predictors stake token for result of a DAO and are rewarded on success and lose their stake on failure.	The upscaling of local majority to global majority is a major disadvantage. There may be use of better predictor stakes and crypto-economic games to transform the opinions.
Permissioned Relative Majority	The algorithm depends on the number of voters voting for and against the proposal. It has simple majority and is less expensive.	With no minimum voting requirement, even a single member can have total power over the decision making.
Quadratic Voting	The voting power is directly linked to the financial power of the node. Offers a solution to risk of relative majority votes and shows how strongly opinionated the community is.	It requires the proof of identity as fake identity could wrongly the influence the voting process.
Proof of Activity	It uses the PoW till the block mining and then shifts to PoS for further incentive distribution.	The system can promote coin hoarding and has high energy consumption. It can also lead to internal conflict.
Proof of Elapsed Time	It Follows a lottery system that spreads the power of voting equally across nodes. The nodes each sleep for a random time and the one with the shortest duration wakes up first to process the block.	It does not truly promote decentralization as it focuses more on the node selection.
Conviction Voting	The token holders use the voting power over the proposals, overtime if the voter stays with the vote, the influence of the vote gets stronger and thus, their proposal accumulates enough votes to pass.	It cannot be used for time-critical decisions.

Table 1. Types of Consensus protocols

V. COMPARATIVE ANALYSIS

Consensus mechanism is at the core of blockchain network, to assess the agreement of the nodes. Proof of Work (PoW), was the earliest mechanism to be implemented in a network, through the block mining process. The expenditure of compute on the node's end to solve a computationally difficult problem makes the cost of a dishonest action exponentially high. The major drawback is the loss of compute power for multiple miners for unrewarded purposes. While Proof of Stake (PoS) works by allowing the nodes to stake in the system, the higher the stake , the greater the reward. It has validators to validate a transaction rather than miners. The validators are selected randomly between the stakers and the person with the highest stake is usually chosen. The validator doesn't receive his stake back, this process is called slashing. It reduces on wasted compute resources, by focusing on the stake of tokens in the network. PoW requires heavy starting investment, whereas PoS can be done with marginal requirements too. PoS is more decentralized than PoW due to easy staking of coins. PoW rewards the miners with coins as well as transaction fees, while PoS returns only

transaction fees to the validators. PoW has higher energy wastage as compared to PoS. Though, the drawbacks are evident but PoW is a tested and robust mechanism that has already been accepted and well received by the crypto industry.

Proof of Burn (PoB), takes investment from the nodes in the form of network tokens. These tokens are sent to a publicly verifiable address, where the coins once sent become inaccessible to the nodes, thus, the burn concept. The higher the amount of burn by a node, greater are it's chances to commit a block to the blockchain. Since, the burn decreases the availability of the coins in the network, it increases the overall value of the withheld coins. In comparison to PoW concept, it consumes less power and energy of the nodes. The differentiating factor for PoS and PoB is the temporary unavailability of the coins in the earlier one, and the permanent destruction of coins in the later one. This mechanism looks for long term commitment from the nodes in exchange of short-term losses to the network.

Proof of Activity (PoA) is a composite mechanism of PoW and PoS. It allows the miners to generate a block through complex problem solving, requiring high-cost equipment. The block once generated has to then be verified by the validators, who are chosen on the basis of the coin percentage held in the network. These validators approve the block and allow for its addition to the network. This mechanism is a fool-proof method as it has double protection mechanism against bad actors of the network. Firstly, when generating a block, for a bad actor to influence, it should hold more than 50% of the network's computational power. Secondly, during the validation , a node must hold more than 50% of all the cryptocurrency in the network for it to overpower the network consensus.

Proof of Elapsed Time (PoET) is implemented only in permissioned networks, where each node's entry to the network is validated by other nodes. The mechanism ensures equal chance to participate in block creation to every node by randomly distributing waiting times to all nodes. The major factor PoET has to look out for is the random distribution , so that no node faces bias and receives the shortest time continuously. It saves on the compute resources compared to PoW and use of coins as compared to PoS. The main concern of identity of node is solved by being implemented only in a permissioned network.

Holographic consensus is the newer generation of mechanism that focus on resilience and scalability of the network. It is usually implemented with the Genesis protocol. It allows user to propose a proposal which has to be passed with an absolute majority , but if certain conditions are met it can be boosted to relative majority. People are allowed to bet their tokens on predicting whether a proposal will pass or not. It leads to a prediction market scenario.

Permissioned Relative Majority has no minimum voting requirements and even a single member can solely pass the proposal. It is different from Holographic consensus where a majority is required to proceed. It is less expensive but may result in a member gaining absolute power over the network.

Quadratic consensus mechanism links the voting power directly with the financial power. Every member has equal right to vote for the proposal. The cost of a vote is the square of the number of votes a member wishes to acquire. Fake identities are overcome by proof of identity which is a basic necessity of quadratic mechanism. Whereas, Conviction mechanism uses time as a utility. Members are allowed to vote on different proposals and the attention for which the member's vote stays in the network. It is a highly efficient mechanism to maintain the power with the elder nodes rather than giving excess power to the newer nodes.

VI. DISCUSSIONS AND FUTURE SCOPE

Consensus mechanism is the core of any blockchain network, they form a base for the agreement of peers in the system. The area of consensus mechanisms came more into limelight with the advent of Decentralized Autonomous Organizations (DAO). These organizations were built around the concepts of a community coming together to work for a common goal and vision.

Bitcoin blockchain introduced by Satoshi Nakamoto had the tokens called as bitcoins which governed the network. The owners of these tokens could perform transactions as well as mine for more incentives through proof-of-work consensus. This consensus mechanism was useful for the system Nakamoto proposed but in general it had the drawback of excess wastage of computation power by other competing nodes who weren't able to win the race to mining.

With this came the next generation of consensus protocols based on proof of stake, where each node could stake a set of network tokens to win the race for mining and would result in lesser loss of computation resources of the network nodes. In 2016, The DAO[13], an organization built on the Ethereum mainnet emerged as one of the first hedge fund communities. The code had a reentrancy bug which was later exploited by a hacker, which questioned the immutability of the chain.

The newer consensus protocols such as Holographic consensus and meritocratic systems focus more on the scalability of the organizations. These mechanisms bring in the specificity of the use case they are being used for. The applications such as DAO-Stack uses Holographic consensus, DAOhaus uses Moloch DAO infrastructure.

With the diversity of consensus protocols[refer Table 1], comes the drawbacks for each. The major application areas of these consensus protocols on the wider spectrum can be seen in e-governance dapps, where voting is done on mass levels and reaching a consensus is the main aim of the application. They can also be used in other areas such as supply chains, hedge funds and other autonomous investing organizations.

The future of this technology can lie in creating distributed applications for better reach of governance to remote areas, through decentralized networks. It can lead to inclusiveness of people and their opinions on major or minor decisions. The technology unlocks a new chapter in the history of governance and democracy.

Consensus mechanism as a standalone technology has a diverse future ahead of it, as all Web3 applications stem from the fact of decentralization and for decentralization to hold true, consensus is a critical point. Consensus mechanism can have a future in the Prediction markets or online re-sale platforms where there has to be some confidence in the product being displayed for the user to purchase it. A

blockchain based solution can be proposed with consensus mechanism to keep valid tracks of items and build more on honest nodes.

Though multiple Industries are using these technology while being crypto-currency centric, but the core fundamentals of blockchain, consensus mechanisms as well as mining functionality can open doors to a new era of autonomous and decentralized organizations, which can lead to a huge disruption in the current e-commerce markets as well as online transaction platforms. It is not only limited to these industries, the disruptions will occur across every platform with middle-men services or a centralized body control, such as organizations or systems.

REFERENCES

[1] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.

[2] Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.548

[3] Hassan, Samer; De Filippi, Primavera (2021) : Decentralized Autonomous Organization, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, Iss. 2, pp. 1-10, https://doi.org/10.14763/2021.2.1556.

[4] Morrison, Robbie & Mazey, Natasha & Wingreen, Stephen. (2020). The DAO Controversy: The Case for a New Species of Corporate Governance?. Frontiers in Blockchain. 3. 25. 10.3389/fbloc.2020.00025.

[5] De Filippi, Primavera and Mannan, Morshed and Reijers, Wessel, The Alegality of Blockchain Technology (December 10, 2021). Policy and Society, Forthcoming , Available at SSRN: https://ssrn.com/abstract=4001696

[6] Xiao, Yang & Zhang, Ning & Li, Jin & Lou, Wenjing & Hou, Y.. (2019). Distributed Consensus Protocols and Algorithms. 10.1002/9781119519621.ch2..

[7] Buterin, V. (2013). Ethereum Whitepaper.

[8] W. Wang et al., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," in IEEE Access, vol. 7, pp. 22328-22370, 2019, doi: 10.1109/ACCESS.2019.2896108.

[9] Muratov, Fedor & Lebedev, Andrei & Iushkevich, Nikolai & Nasrulin, Bulat & Takemiya, Makoto. (2018). YAC: BFT Consensus Algorithm for Blockchain.

[10] Faqir, Youssef & Arroyo, Javier & Hassan, Samer. (2020). An overview of decentralized autonomous organizations on the blockchain. 1-8. 10.1145/3412569.3412579..

[11]https://hyperledgerfabric.readthedocs.io/en/latest/ledger/ledger.html#blocks

[12] Monrat, Ahmed Afif & Schelén, Olov & Andersson, Karl. (2019). Survey of Blockchain from the Perspectives of Applications, Challenges and Opportunities. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2936094..

[13] Morrison, Robbie & Mazey, Natasha & Wingreen, Stephen. (2020). The DAO Controversy: The Case for a New Species of Corporate Governance?. Frontiers in Blockchain. 3. 25. 10.3389/fbloc.2020.00025....

[14] Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Weili & Chen, Xiangping & Weng, Jian & Imran, Muhammad. (2019). An Overview on Smart Contracts: Challenges, Advances and Platforms..

[15] N. Diallo et al., "eGov-DAO: a Better Government using Blockchain based Decentralized Autonomous Organization," 2018 International Conference on eDemocracy & eGovernment (ICEDEG), 2018, pp. 166-171, doi: 10.1109/ICEDEG.2018.8372356..

[16] Norta, Alex. (2015). Creation of Smart-Contracting Collaborations for Decentralized Autonomous Organizations. 10.1007/978-3-319-21915-8_1..

[17] Viriyasitavat, Wattana & Hoonsopon, Danupol. (2018). Blockchain Characteristics and Consensus in Modern Business Processes. Journal of Industrial Information Integration. 13. 10.1016/j.jii.2018.07.004..

[18] Ziolkowski, Rafael & Miscione, Gianluca & Schwabe, Gerhard. (2020). Exploring Decentralized Autonomous Organizations: Towards Shared Interests and 'Code is Constitution'..

[19] Hewa, Tharaka & Hu, Yining & Liyanage, Madhusanka & Kanhare, Salil & Ylianttila, Mika. (2021). Survey on Blockchain-Based Smart Contracts: Technical Aspects and Future Research. IEEE Access. 10.1109/ACCESS.2021.3068178..

[20] Cachin, Christian & Vukolic, Marko. (2017). Blockchains Consensus Protocols in the Wild.

[21] Rikken, O., Janssen, M., & Roosenboom-Kwee, Z. (2019). Governance challenges of blockchain and decentralized autonomous organizations. Information Polity, 24(4), 397-417. https://doi.org/10.3233/IP190154.