Relative Study of Consensus Algorithms in Blockchain

Varun Prakash[1] Saksham Chawla[2] Suman Tripathy[3] Sunny Arora[4]
[4]Assistant Professor
[1,2,3,4]Department of Computer Science Engineering
[1,2,3,4]Dr. Akhilesh Das Gupta Institute of Technology & Management, New Delhi, India

Abstract— Consensus is a central issue of distributed computing. Today, with the new coming of blockchains, different consensus executions were proposed to settle on copies agree on the request for exchanges updating what is called a distributed ledger. Being a distributed ledger, consensus mechanism is needed among peer nodes of a blockchain network to ensure its proper working. In this paper, we examine the standard blockchain consensus calculations and we have distinguished and examined boundaries identified with execution and security of consensus in blockchain. Specifically, we talk about proof of work consensus and show the contrasts between the Bitcoin and the Ethereum verification of work consensus calculations.

Keywords: Blockchain, Bitcoin, Distributed Ledger, Consensus

I. Introduction

Blockchain innovation arose to beat the dangers and shortcomings in business transactions. It has revolutionized the structure of industries and businesses by fundamentally changing the way people and organizations trade computerized resources and tracking ownership of these assets without the control of a central authority [1] [2]. Blockchain can be characterized as a distributed ledger, divided between the nodes of a business network. Transactional information is stored in blocks connected to one another shaping a chain. Each transaction is verified by the majority of participants of the system. It contains every single record of each transaction.

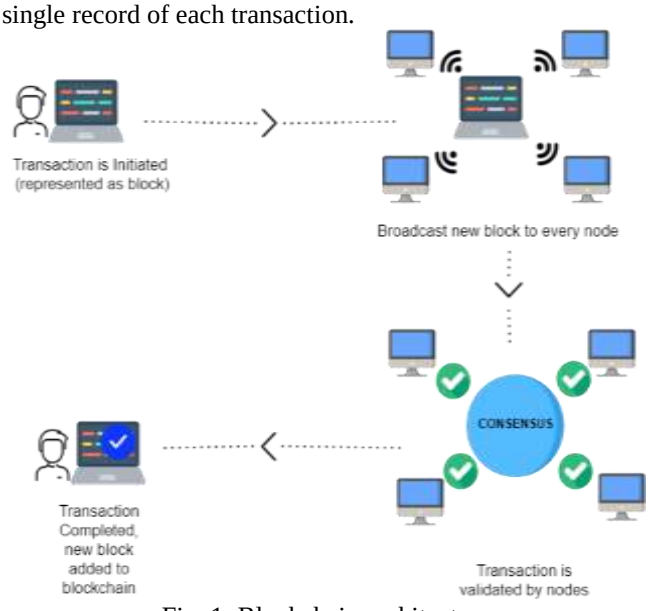

Fig. 1: Blockchain architecture

When contrasted with conventional distributed databases, blockchain has a significant edge in terms of Transparency, Security and Flexibility [3].

Blockchain utilizes a consensus convention among nodes of the network to approve the data, disposing of the requirement for intermediaries. Consensus mechanism in blockchain guarantees an alter free climate in which only one variant of truth is settled upon by all the nodes. Every one of the nodes in a decentralized network should agree about condition of the blockchain. This makes it hard for an attacker to alter a block in the blockchain. Choosing the correct consensus calculation is an essential choice to make while carrying out a blockchain arrangement. Each of the most popular blockchain platform, Bitcoin, Ethereum, varies in aspects of decentralization, permission, anonymity, and native-currency, and has its own consensus mechanism, algorithm and implementation

Various consensus algorithms designed for blockchain are reviewed in this paper considering parameters relevant to consensus algorithm.

II. Blockchain and Consensus Mechanism

Blockchain could be viewed as a public ledger, wherein all dedicated transactions are stored in a chain of blocks. This chain consistently grows when new blocks are annexed to it. The blockchain technology has the key attributes, such as decentralization, persistency, anonymity and auditability. Blockchain can work in a decentralized environment, which is enabled by integrating several core technologies such as cryptographic hash, digital signature (based on asymmetric cryptography) and distributed consensus mechanism. Each block points to the promptly previous block through a reference that is essentially a hash value of the previous block called parent block. The first block of a blockchain is called *genesis block* which has no parent block.

Consensus means to reach agreements among network nodes or systems, according to the interest of the system participants [4]. In blockchain, how to reach consensus among the nodes is a transformation of the Byzantine Generals Problem. Consensus is a center idea in distributed systems and not confined to blockchain. Figure 2 depicts the architecture of blockchain. It applies to situations in which various processes or nodes need to keep a typical state of data item. Permission-less and permissioned blockchain are two significant sorts of blockchain. In permission-less blockchain, nodes are anonymous. Another altered exchange block can be added bringing about a fork. Fork happens where a legitimate exchange confuses with the invalid one. The essential objective of consensus calculation is to accomplish understanding among the nodes to such an extent that every node concedes to one genuine worth. In permissioned blockchain, the nodes are not anonymous and considered as known entities. In general, consensus is worth to consider where the nodes of a network are faulty or they communicate in an unreliable way.

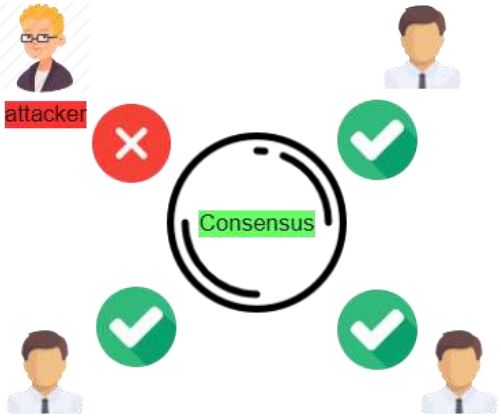

Fig. 2: Consensus Architecture

III. Cryptocurrencies and Consensus Implementations

Trade on the Internet has come to depend only on monetary organizations filling in as confided in outsiders to deal with electronic installments. While the framework functions admirably enough for most transactions, it actually experiences the innate shortcomings of the trust based model. Totally non-reversible transactions are not actually conceivable, since monetary organizations can't try not to intervene debates. The expense of intervention expands exchange costs, restricting the least down to earth exchange size and removing the opportunities for little easy-going transactions, what's more, there is a more extensive expense in the deficiency of capacity to make non-reversible installments for nonreversible administrations. With the chance of inversion, the requirement for trust spreads. Dealers must be careful about their clients, bothering them for more data than they would somehow or another need. A specific level of misrepresentation is acknowledged as unavoidable. These expenses and installment vulnerabilities can be kept away from face to face by utilizing actual cash, yet no component exists to make installments over a correspondences channel without a confided in party. What is required is an electronic installment framework dependent on cryptographic verification rather than trust, permitting any two agreeable partakers to execute straightforwardly with one another without the requirement for a trusted outsider. Transactions that are computationally illogical to opposite would secure dealers from misrepresentation, and routine escrow components could undoubtedly be executed to secure purchasers.

A. Bitcoin

In Bitcoin, a transaction is an atomic activity that addresses the transaction of money from sender to beneficiary. A transaction is distinguished by its hash value. For carefully marking the transaction, a private key is utilized. Public key is utilized in verification of the transaction. Every node in this organization has a duplicate of the ledger. To execute a distributed timestamp server on a peer to peer premise a proof of-work framework is utilized. The proof of work includes examining for a worth that when hashed, for example, with SHA-256, the hash starts with various zero bits. Miners in a blockchain should confirm the transaction and sender's public key based signature. They need to perform hefty calculation to demonstrate that they are valid entities in the network. Merkle trees are used in Bitcoin to check and submit transactions. It is a binary hash tree where each leaf holds transaction's ID and is addressed by hash of its child nodes. A transaction is submitted with a solitary hash value stored at the root of Merkle tree. Every user need to store just the root node of the Merkle tree.

1) Implementation

The Bitcoin consensus source code [5] is depicted in figure 3.

Fig. 3: Bitcoin Consensus Implementation

B. Ethereum

Ethereum was introduced to overcome drawbacks of Bitcoin. The blocks in Ethereum also hold a list, Ethereum also ensures execution of smart contracts. It uses GHOST protocol to ensure consensus in the network. It addresses the issue of stale blocks that arise when a group of miners possess more computation power than the rest and thus contribute more to the network. This will result into centralization issue. The GHOST protocol integrates the stale blocks in longest blockchain calculation. The stale blocks are rewarded that eliminates the centralization issue. As compared to Bitcoin, Ethereum has better block time (15 seconds).

1) Implementation

The Ethereum consensus source code [6] is depicted in figure 4.

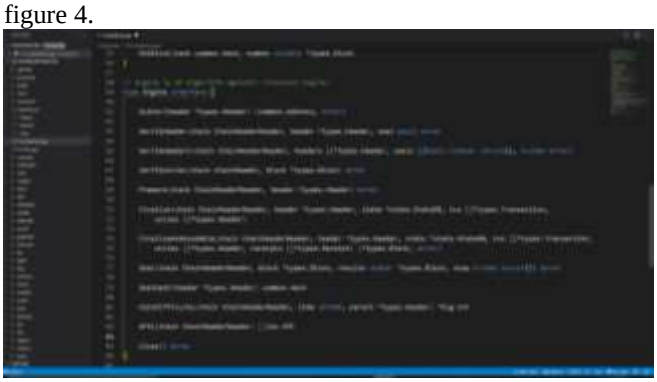

Fig. 4: Ethereum Consensus Implementation

IV. Relative Analysis Of Consensus Algorithms in Blockchain

This section discusses the parameters relevant in evaluating the consensus algorithms in blockchain. Scalability, Latency, Types, attacks, energy consumption, mining, consensus category, and consensus finality are identified as a critical parameters for comparing the various consensus algorithms for blockchain. Comparative analysis of some

recently proposed algorithms: leader-free Byzantine consensus [7], implicit consensus [8], blockchain with unbounded throughput [8], Proof of trust (PoT) [9], DBFT consensus [10], PoPF [11], Ripple [12], Proof of Vote [13], and Proof of work [14] is performed. The relative analysis is presented as under.

- *Scalability:* Scalability is a core requirement to deal with big data in today's environment. Scalability is achieved if increasing the number of nodes results in more transaction blocks being processed. Proof of trust is scalable. Implicit consensus and PoW are not scalable solutions. Other algorithms involved in analysis are not tested with respect to their scalability yet.
- *Types:* There are three types of blockchain, public, private, and consortium [15]. The type of blockchain defines the membership control in the consensus algorithm. This has to be considered while evaluating the consensus algorithms to check what kind of membership is assumed in the design.
- *Vulnerability:* Ripple is prone to Sybil attack in which single attacker controls multiple network nodes by creating different IP addresses, Leader free consensus, PoT are secure against this attack.
- *Energy Consumption:* The energy consumption of almost the entire consensus algorithm is not practically calculated.
- *Mining:* It defines how the process of mining is carried out in the blockchain network. Proof-based consensus is ideal for networks with large number of nodes. Vote-based consensus, on the other hand, works best with limited number of nodes.

Consensus algorithms	**Parameters**				
	Scalability	***Blockchain type***	***Prone to attacks***	***Energy consumption***	***Mining***
Leader- free Byzantine Consensus	-	consortium	-	-	Non-proof of work based mining
Implicit Consensus	Not Scalable	permissioned	DDoS attack	-	Proof based mining
Proof of trust (PoT)	Scalable	Permission-based consortium	DDoS attack	-	Probability and vote based mining
DBFT Consensus Algorithm	-	permissioned	-	-	Non-proof of work based mining (random selection of verifier)
PoPF	-	permissioned	-	Less energy consumption claimed as compared to PoW	Selection on the basis of accounting right
Ripple	-	permissioned	DoS attack, Sybil attack	-	Vote based mining
Proof of Vote (PoV)	-	consortium	-	-	Vote based mining
Proof of Work (PoW)	Not Scalable	Permission-less	Selfish mining, DoS attack, Sybil attack, bribe attack	538 KWh electricity consumption	Based on computational power

Table. 1: represents relative analysis of Different Consensus algorithms

V. Conclusion

In this paper, we have talked about the consensus mechanism, their categories, and significance in distributed environment. Consensus components are talked about by and large for a distributed network and explicitly for blockchain. We contrasted some as of recently proposed consensus algorithms with respect to number of parameters that have a huge effect on consensus algorithm. The parameters recognized for correlation covers both security and execution angles. The algorithms are then examined alongside each of the recognized parameters.

References

[1] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," Applied Innovation, vol. 2, pp. 6–10, 2016.

[2] M. Pilkington, "11 blockchain technology: principles and applications," Research handbook digital transformations, p. 225, 2016.

[3] T. McConaghy, "Blockchain, throughput, and big data," Bitcoin Startups Berlin, Oct, vol. 28, 2014.

[4] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. J. Kishigami, "Blockchain contract A complete consensus using blockchain," in Consumer Electronics (GCCE), 2015 IEEE 4th Global Conference on. IEEE, 2015, pp. 577–578.

[5] The Bitcoin Core developers. Bitcoin Core source code. https://github.com/bitcoin/bitcoin.

[6] The go-ethereum Authors. Go Ethereum. https://github.com/ethereum/go-ethereum.

[7] T. Crain, V. Gramoli, M. Larrea, and M. Raynal, "(leader/randomization/signature)-free byzantine consensus for consortium blockchains," arXiv preprint arXiv:1702.03068, 2017.

[8] Z. Ren, K. Cong, J. Pouwelse, and Z. Erkin, "Implicit con- sensus: Blockchain with unbounded throughput," arXiv preprint arXiv:1705.11046, 2017.
[9] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li, "A proof-oftrust consensus protocol for enhancing accountability in crowdsourcing services," IEEE Transactions on Services Computing, 2018.
[10] S. Jeon, I. Doh, and K. Chae, "Rmbc: Randomized mesh blockchain using dbft consensus algorithm," in. Information Networking (ICOIN), 2018 International Conference on. IEEE, 2018, pp. 712–717
[11] X. Fu, H. Wang, P. Shi, and H. Mi, "Popf: A consensus algorithm for jcledger," in Service Oriented System Engineering (SOSE), 2018 IEEE Symposium on. IEEE, 2018, pp. 204–209.
[12] D. Schwartz, N. Youngs, A. Britto et al., "The ripple protocol consensus algorithm," Ripple Labs Inc White Paper, vol. 5, 2014.
[13] K. Li, H. Li, H. Hou, K. Li, and Y. Chen, "Proof of vote: A highperformance consensus protocol based on vote mechanism & consortium blockchain," in High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2017 IEEE 19th International Conference on. IEEE, 2017, pp. 466– 473.
[14] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[15] "Different types of blockchains in the market and why we need them," [online] https://coinsutra.com/different-types-blockchains/.

