Clustering Based Consensus Algorithm

Nikhil Verma
Information Technology
National Institute Of Technology
Karnataka, Surathkal,India 575025
nikhilverma.222it026@nitk.edu.in

Neeraj Kumawat
Information Technology
National Institute Of Technology
Karnataka, Surathkal, India 575025
neerajkumawat.222it023@nitk.ac.in

***Abstract*— The Practical Byzantime Fault Tolerance(pBFT) Algorithm and Raft consensus algorithm does not scale well because of its communication overhead. As the number of nodes increases so does the time takes to respond to a request. And pBFT does not take into account how much stake a node has in the blockchain. Also to select a new leader there is communication overhead. In this paper we are proposing a consensus algorithm based on clustering of nodes to form a primary group of nodes. This primary group will elect a node among themselves as leader to add blocks to the blockchain. The formation of cluster and selection of member of the primary group of nodes is based on the stake of nodes on the chain. Theoretical analysis shows that our proposed consensus algorithm can optimize the selection of the leader to mine a block.**

Keywords*— *Blockchain, consensus, Byzantime fault.

I. INTRODUCTION

Blockchain technology was introduced with the introduction of Bitcoin. The technology behind the Bitcoin already existed before but the consensus mechanism was new to the bitcoin. Blockchain is essentially a distributed and append only ledger. It integrates multiple technology such as distributed ledger, decentralized decision making, cryptography, consensus mechanism to achieve transparency, credibility and immutability. Based on deployment blockchain are classified into public blockchain and private blockchain. In public blockchain any node with internet access can join the blockchain and submit transaction and participate in mining. Identity of nodes in public blockchain are not known to other nodes (eg. Bitcoin, Etherium). In private blockchain node usually identity of nodes are known and there is verification process to join the blockchain (e.g. Supply Chain Management, Healthcare).

Consensus mechanism is a core component of blockchain, which directly affects the efficiency and scalability of the blockchain. A blockchain consensus mechanism denotes how to make mutually distrusting nodes agree on a new block periodically to be added to the blockchain , which should meet the basic properties, : (a) consistency: all nodes should agree on a same block; (b) Validity: a decided block should be proposed by a consensus node; (c) liveness: every normal node should eventually decide some block. The consistency and validity properties define the safety property of the blockchain consensus.

According to the different deployment types of blockchain, existing blockchain consensus algorithm can be roughly be divided into proof-of-concept based and voting based. The proof of concept based consensus such as proof of work, proof of stake are appropriate for public blockchain, which suffer from low efficiency and high computational power. The voting based consensus algorithm such as BFT consensus algorithm, Raft, stellar, ripple are usually used in private blockchain. However, most of exiting BFT-type consensus algorithms are either with low scalability, e.g. the performance of PBFT consensus algorithm will decline sharply with the increase of the number of nodes, or with a low Byzantine fault-tolerant rate. In this paper, we propose a new consensus mechanism based on the transaction history between nodes creates a primary group, which narrows the consensus nodes down to a group of nodes with higher stake in the blockchain.

Overall, the main contributions of this paper are summarized as follows –

- We propose a transaction history based mechanism to build a trustworthy consensus group with higher stake in the Blockchain. It an prevent the nodes with lower trust values from participating in consensus, narrows down the number of consensus consortium nodes and improves consensus efficiency
- We propose method of selecting a leader among the primary group which prevents any node from always being selected as leader and gives fair chance to member of the primary group to become the leader.
- We will analyse our algorithm for efficiency, scalability, fairness.
- We explain how our algorithm will handle problems such as Byzantine general problem, node failure.

II. PRIVATE BLOCKCHAIN CONSENSUS ALGORITHMS

Blockchain consensus refers to the mutual distrust nodes come to an agreement on a new block that will be appended to blockchain in a distributed environment, which has been received extensive attentions. We have analyzed published research based on consensus algorithm for private blockchain.

1. Practical Byzantine Fault Tolerent Algorithm – the pBFT: Nodes in a pBFT enabled system are sequentially ordered with one node being the primary (or the leader node) and others referred to as secondary (or the backup nodes). Note here that any eligible node in the system can become the

primary by transitioning from secondary to primary (typically, in the case of a primary node failure). The goal is that all honest nodes help in reaching a consensus regarding the state of the system using the majority rule.

Major features of pBFT consensus are it's energy efficiency, it achieves consensus without carrying out complex mathematical computation. Another feature of pBFT are transaction finality i.e. the transactions do not require multiple confirmations (like in case of POW mechanism in Bitcoin). in pBFT Every node in the network takes part in responding to the request by the client and hence every node can be incentivized leading to low variance in rewarding the nodes that help in decision making.

Limitations of pBFT are scalability, pBFT does not scale well because of its communication (with all the other nodes at every step) overhead. As the number of nodes in the network increase (increases as O(n^k), where n is the messages and k is the number of nodes), so does the time taken to respond to the request.

2. Raft Consensus Algorithm - Raft states that each node in a replicated state machine (server cluster) can stay in any of the three states, namely, leader, candidate, follower. In Raft consensus leader is selected by election. In the election process some of the follower volunteer to become leader and request vote from the follower through request message. Followers vote for suitable candidate and based on the majority of the voted a leader is selected. And only leader is allowed to append the ledger.

   Major features of Raft Consensus are the system following the Raft consensus protocol will remain operational even when minority of the servers fail. Another feature of Raft is that each node has a fair chance to become a leader.

   Limitations of Raft Consensus is it's scalability because Raft is a single leader protocol and every transaction goes through the leader. As the blockchain expands and number of transaction grows traffic through leader increases which can choke the system.

3. Stellar Consensus Algorithm – Stellar consensus algorithm is based on Federated Byzantine Agreement consensus mechanism. In FBA systems, each node does not have to be known and verified ahead of time, membership is open, and control is decentralized. Nodes can choose whom they trust. System-wide quorums emerge from decisions made by individual nodes.

   Major features of FBA are the ability to choose whom each node trusts which decentralizes the trust in the Blockchain. And individual node trust can be based on different criteria.

   Limitations of Stellar Consensus are that there can be cascading failure has a significant impact on the Stellar system. In fact, the entire system can fail completely in sequence if only the two nodes operated by the Stellar foundation are deleted.

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the A4 paper size. If you are using US letter-sized paper, please close this file and download the Microsoft Word, Letter file.

III. Proposed Methodology

1. **Node Importance Evaluation** – in our proposed consensus mechanism each node in the blockchain are assigned a weight parameter. The high value of the weight parameter implies high importance of the node in the blockchain.
   - Initially we assign same weight to each node which is equal to 1/N. where N is the total number of nodes the blockchain.
   - Weight of a node is multiplied by how many nodes it has direct transaction with.
2. **Node Clustering -** In Our proposed consensus mechanism we are creating clusters of node which are directly related. Two nodes are considered related if they have direct transaction with each other. We are also putting a minimum cluster size K1 to prevent large number of cluster formation and large number member in the primary group. And we also putting limit on the maximum cluster size K2 to prevent formation on only one cluster if all the nodes have direct transaction with each other. The parameters K1 and K2 can be changed according to the size of the Blockchain network.

   Clustering Algorithm-

   Input: Node i , node set with N nodes

   Output: node set of a cluster

   1. If Nodei. Clustered = True:

   return

   2. add node i to cluster set

   3. For every node j in node set do

   If node j does direct transaction with node i then and cluster set length is less than K2:

   Add node j to cluster set

   node j. clustered = True

   4. If size of cluster set is less than K1 then:

   For all node in cluster set node.clustered = False

   Return Empty

   5. Else Return cluster set
3. **Selecting Member for primary group –** From every cluster we are selecting a node with highest weight as leader of the cluster who will be a member of the primary group.

4. **Selecting a leader among primary group –** a node who is member of the primary group will be selected to add block to the blockchain. There will a voting process for selection of the leader. The rules and steps for voting are as follows:
    - A member cannot vote for himself
    - Identity of a member are not known to other member.
    - Member with highest vote will be selected as leader who will mine block.
    - Selected leader's tenure will be for mining some blocks.
    - After the tenure of the leader has ended again voting will be conducted to select a new leader.
    - In the next round of voting vote towards the previous leader will not be counted. So even if every member votes same as before the member with highest vote other than previous leader will be selected as leader.
    - Vote towards previous leader will not be counted for a fix rounds of voting.
5. **Reclustering –** As new transaction are made with addition of new blocks the clustering process will be performed in some interval to take new transaction into account for selecting the leader. if more than half of the primary node member fails we perform reclustering.
6. **Initialization –** initially all node will be considered in the primary group. And after one round clustering will be performed based on the transactions.

IV. Analysis of the Proposed Algorithm

1. **Effectiveness –** Our proposed consensus algorithm is a multistage consensus algorithm, which is based on PBFT. Our proposed algorithm is different from PBFT in the following aspects that the nodes with high direct transaction rate will be more trustworthy at a high probability driven by personal interests and profits. We reduce the risk of single view change process by replacing the single primary node with primary group. In the primary group we use group signature to enhance anonymity of the primary group member nodes, which can reduce the probability of these nodes being attacked.

2. **Efficiency –**

I. *Number of messages delivered*: In our T-PBFT, the consensus process is limited within the bounds of primary group members rather than all the nodes in Nodes. Apparently, the number of messages during the consensus process is reduced. Assume that the total number of nodes in the blockchain system is N. assume that d (N/K1< d <N/K2) nodes participate in the consensus process. The number of messages will be O(d^2). Thus it can be seen that the communication complexity is reduced.

II. *Byzantine fault tolerance:* As we all know, the Byzantine fault-tolerant rate of PBFT algorithm is (N-1)/3. In our T-PBFT, the Byzantine fault-tolerant rate will be optimized. The system selects d node to the primary group, the nodes excluded from the primary group will have no effect on the consensus process. If f is the number of byzantine node in the primary group then to become a leader a node needs to receive votes from at least two members. So maximum number of byzantine nodes inside the primary group is one. And maximum number of byzantine nodes outside the primary group is N-d. thus from the aspect of the whole system number of byzantine node in the system is the sum of maximum number of byzantine node inside the primary group and outside the primary group. that is (N-d+1).

3. **Scalability -** As we all know, most of the consensus algorithms based on Byzantine fault tolerance have poor scalability. When the number of nodes in the algorithm reaches a certain scale, the performance will drop sharply. In our proposed clustering based consensus algorithm, we do not limit the number of the nodes in the system, but by introducing the clustering of directly related nodes and setting of the primary group, we can reduce the number of the nodes that participate in the consensus process. This will make our algorithm more suitable for a large-scale network environment.

4. **Size Of Primary Group** – Based on the size of the network max cluster can be fixed to limit the size of the primary group.

V. Conclusion

Size of the private blockchain network will depend on the requirements of the organization. Our proposed algorithm can be deployed both in environment with less number of node or in environment with very large number of node. In our proposed algorithm we are trying to reduce the communication overhead required for consensus, size of the cluster will be changed according the size of the network. This will keep number of message passed during voting in the primary group irrespective of the size of the network.

References

[1] Wu, Yusen, et al. "The research of the optimized solutions to Raft consensus algorithm based on a weighted PageRank algorithm." *2022 Asia Conference on Algorithms, Computing and Machine Learning (CACML)*. IEEE, 2022.

[2] S. Pahlajani, A. Kshirsagar and V. Pachghare, "Survey on Private Blockchain Consensus Algorithms," 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), 2019, pp. 1-6, doi: 10.1109/ICIICT1.2019.8741353.

[3] D. Huang, X. Ma and S. Zhang, "Performance Analysis of the Raft Consensus Algorithm for Private Blockchains," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, no. 1, pp. 172-181, Jan. 2020, doi:1109/TSMC.2019.2895471

.