CLUSTERING BASED CONSENSUS ALGORITHM

An hybrid consensus approach based on Raft algorithm and node transaction history

Presented By :
Nikhil Verma (222IT026)
Neeraj Kumawat (222IT024)

INTRODUCTION

- The Raft consensus algorithm does not scale well because of its communication overhead. Also this algorithms does not consider the stake of node during consensus. We are proposing consensus algorithm based on connectivity of nodes, which is determined by transaction between nodes.

METHODOLOGY

- In our proposed algorithm we are assigning weights to each node which denotes the node's importance or stake in the blockchain.
  - Weight of a node is calculated based on how many nodes it transacts.
  - Initially each node has weight of 1/N, where N is the total number of nodes in the blockchain.
  - Weight of a node will be multiplied by the number of nodes it has directly done transaction previously.

- **Clustering Of Nodes** – node with direct transaction are clustered into a group. We are putting minimum and maximum group size limit to prevent formation of large number of cluster and having only one cluster respectively.
- We select one member from each cluster with highest weight as member of primary group. If members in a cluster have same weight then we select member with more total number of transaction. If they have same no of transaction we select one member among them randomly.

METHODOLOGY CONTD.

- There will a voting process to select a leader among the members of the primary group. The rules of selecting a leader are:
  - A member cannot vote for himself.
  - Identity of members are will be anonymous to the other members to reduce the probability of attack on nodes.
  - Members of the primary group will vote for selecting a leader.
  - The member with highest votes will be selected as leader and will be allowed to mine blocks.
  - For mining a block the leader will receive incentive.
  - The leader's tenure will be some fix number of block.
  - When the leader's tenure has expired again voting will be conducted to select a new leader.
  - For next fix number of rounds voting towards the previous leader will not be counted and the member who receive next highest vote will become the leader.
  - This will reduce the risk of malicious node.

METHODOLOGY CONTD.

- As new transaction are made with adding new block to the blockchain, the clustering process will be performed at some fix time interval to update the primary group according to the state of the network.
- When initializing the blockchain all node will be considered in primary group.

CLUSTERING ALGORITHM

Input: Node $_i$, node set with N nodes

Output: node set of a cluster

1. If node(i).clustered = True:
   - Return
2. Add node(i) to Cluster set and update node(i).clustered = True
3. For every node j in node set do:
   - If node(j) does direct transaction with node(i) and cluster set size is less than K2:
     - Add node(j) to cluster set
     - node(j).clustered = True
4. If size of cluster is less that K1 then:
   - For all node in cluster set update node.clustered = False
   - Return
5. Return Cluster set

ANALYSIS

- Effectiveness
  - In our proposed algorithm the node with more transaction will be more trustworthy driven by their stake in the network.
  - We are reducing the risk of malicious node by using primary group of members to select a leader.
  - In the primary group identity of members will be anonymous, which will reduce the risk of attack on nodes.

ANALYSIS CONTD.

- Efficiency
  - Number of messages: as the consensus process is limited within the primary group members, number of messages during consensus process is reduced.
  - Byzantine fault tolerance: as member of primary group are selected based on their transaction history. The node with high transaction will have more stake in the network.
- Scalability –
  - In our proposed cluster 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.

ADVANTAGES

- As number of message to reach consensus is less it is also suitable for large network.
- Reduces the chance malicious node being selected to mine a block.
- As number of message passed to reach consensus is less the transaction will be fast.
- Member in the primary group are selected based on their weight which also represent their stake in the network motivates them keep the network correct and secure.
- Reduces the risk of single member from the primary group being always selected as leader.
- Reduces probability of any with high transactions to gain control by limiting the number of nodes in cluster.

DISADVANTAGES

- Making clusters is an overhead to the network.
- Node with less transaction will not be allowed to mine a block.
- Incentivizes nodes with high transaction history.

THANK YOU