A Proposed Currency System for Academic Peer Review Payments Using the BlockChain Technology

Background

Peer review of scholarly papers is seen to be a critical step in the publication of high quality outputs in reputable journals.

Defects with the mechanism: Bribe, acquaintance in journals, negtive academic rival, etc. They all can affect the justice of the paper contribution.

We aimed at achieving an anonymous paper-review system base on the blockchain mechanism.

My Work

Frame of Blockchain

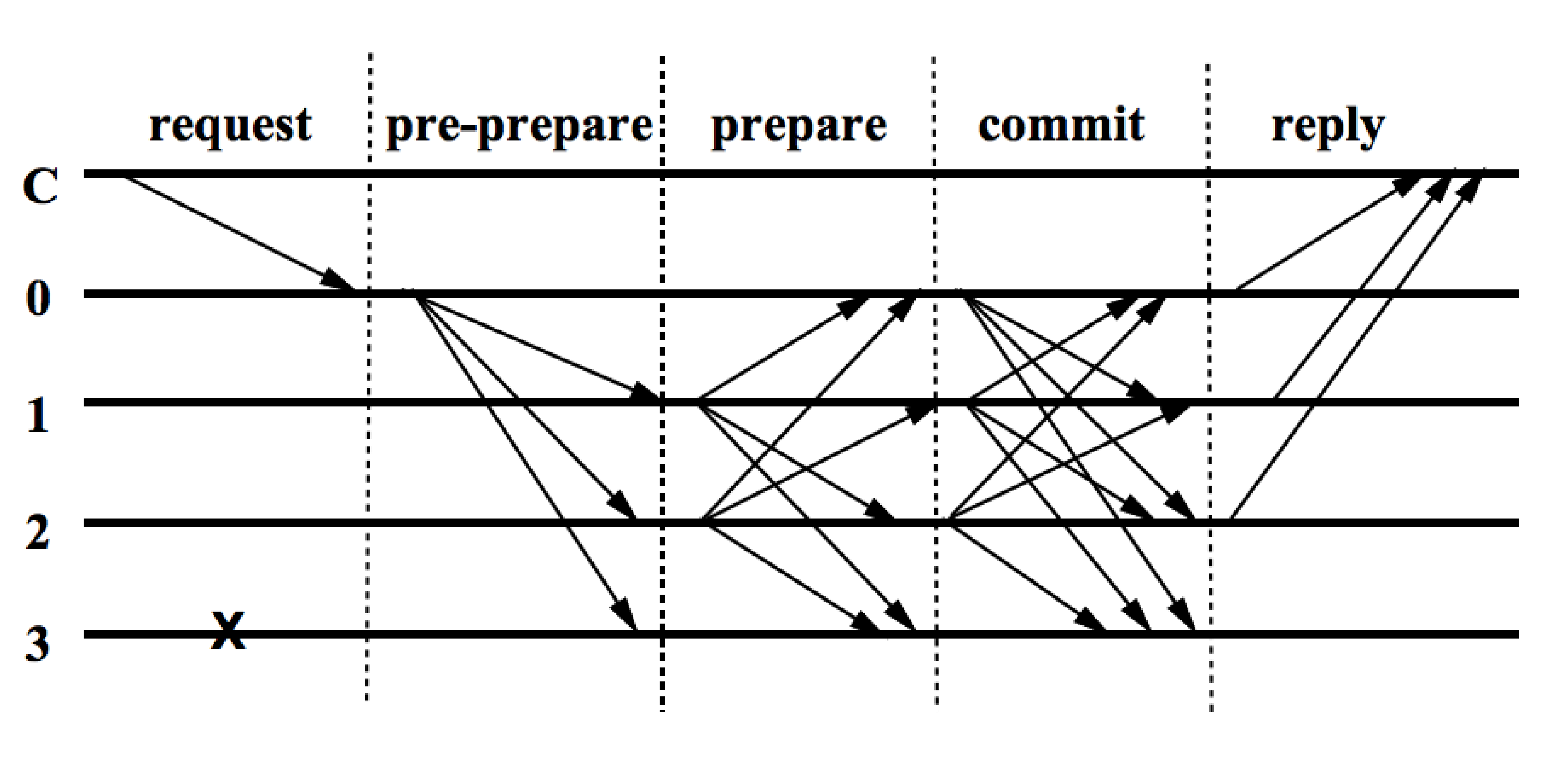
Application layer	Programable Currency, Programable Society...
Protocal layer	Script, Algorithm, AI protocal...
Incentive layer	Issue Mechanism, Distribution Mechanism
Concensus layer	PoW、PoS、DPoS、...
Network layer	P2P Network, Propagation Mechanism...
Data layer	Data Block, Time Stamp, Hash Function, Merkle Tree...

Consensus Layer

Practical Byzantine Fault Tolerance

- A client sends a request to invoke a service operation to the primary
- The primary multicasts the request to the backups
- Nodes execute the request and send a reply to the client
- The client waits for 1 replies from different replicas with the same result;

Practical Byzantine Fault Tolerance



Practical Byzantine Fault Tolerance

Pre-prepare The primary assigns a sequence number, *n*, to the request, multicasts a pre-prepare message with*m* piggybacked to all the backups, and appends the message to its log. The primary tells the backups a protocol is arosen.
Prepare The backups get the message from the primary and check the message is legal. They will multicast to all other replicas and adds both messages to its log. Otherwise,it does nothing. The nodes will accept at least *n*+1 non-faulty messages (the same as itself) . Then they will go to the commit part or just stop here.
Commit The nodes calculate the new block and multicast the new block. If any node in the chain receive at least *n* + 1 blocks as a same block. This block will be written on it blockchain.

Delegated BFT

- Using a ramdom number to decide who is in the congress and suppose that there are $R = 3n + 1$ nodes in the congress, where the n is the maximum of faulty nodes.
- A client multicasts a request of transaction and the every node in the congress log this transaction.
- Once the new block is to be written, the primary multicasts the request to the backups in the congress.

Delegated BFT

- Nodes execute the request also like what PBFT do, at last they multicast the new block to all the node in the network. Every node, receive the new block and wirite it to its own chain.
- If the primary is accused of being faulty, the primary lose its right. After a certain time (or even just change the congress every time we reach the consensus), the division of the two parts of nodes will also alter.

Future work

✓ Using a cryptological method to delegate the vertifier

✓ Implement the system on the existed framework just like Hyperledger

Thanks