

CLAIMS:

1. A computer-implemented consensus method to be implemented on a blockchain maintained by a number (N) of nodes, wherein one of the nodes acts as a primary node and the other (N-1) nodes act as backup nodes, and the method is performed by one of the N nodes, the method comprising:

detecting a change in a current height H of the blockchain;

determining the primary node based on a parameter P and the number of nodes N, wherein the parameter P is proportional to the current height H of the blockchain;

in response to determining that the one of the N nodes is the primary node, executing a Practical Byzantine Fault Tolerance (PBFT) normal operation protocol as the primary node; and

in response to determining that the one of the N nodes is not the primary node, executing the PBFT normal operation protocol as one of the backup nodes.

2. The method of claim 1, wherein:

the current height H is based on a number of blocks in the blockchain; and

the parameter P is identical among a plurality of the N nodes that respectively recognize the same current height H of the blockchain.

3. The method of any preceding claim, wherein:

each of the nodes is associated with an identification; and

determining the primary node based on the parameter P and the number of nodes N comprises: determining one of the nodes that has an identification of $(P \bmod N)$ to be the primary node.

4. The method of any preceding claim, wherein executing the PBFT normal operation protocol comprises:

executing the PBFT normal operation protocol to add a new block to the blockchain.

5. The method of any preceding claim, further comprising:

repeating the steps of claim 1 for one or more rounds of the execution of the PBFT normal operation protocol; and

for each of the one or more rounds, changing the primary node based on the parameter P and the number of nodes N.

6. The method of any preceding claim, wherein detecting the change in the current height H of the blockchain comprises:

detecting that a number of blocks in the blockchain has increased by one.

7. The method of any preceding claim, wherein in response to determining that the one of the N nodes is the primary node, executing a PBFT normal operation protocol as the primary node comprises:

multicasting a pre-prepare message to at least some of the backup nodes;

obtaining (Q-1) or more prepare messages respectively from (Q-1) or more of the backup nodes, wherein the prepare messages each indicate an acceptance of the pre-prepare message by the corresponding backup node, Q (quorum) is $(N+F+1)/2$ rounded up to the nearest integer, and F is $(N-1)/3$ rounded down to the nearest integer;

multicasting a commit message to at least some of the backup nodes, the commit message indicating that the primary node agrees to the (Q-1) or more prepare messages; and

obtaining, respectively from Q or more nodes among the primary node and the backup nodes, Q or more commit messages each indicating that the corresponding node agrees to (Q-1) or more prepare messages received by the corresponding node.

8. The method of claim 7, wherein:

before multicasting the pre-prepare message to at least some of the backup nodes, the method further comprises obtaining one or more transaction requests from at least one of: one or more clients or one or more of the backup nodes; and

after obtaining the Q or more commit messages, the method further comprises packing the one or more transactions into a new block to add to a local copy of the blockchain.

9. The method of claim 7 or 8, wherein:

the Q or more commit messages include the multicast commit message.

10. The method of any of claims 1-6, wherein in response to determining that the one of the N nodes is not the primary node, executing the PBFT normal operation protocol as one of the backup nodes comprises:

- obtaining a pre-prepare message from the primary node;
- multicasting a prepare message to at least some of the primary node and the other (N-2) backup nodes, the prepare message indicating an acceptance of the pre-prepare message;
- obtaining (Q-1) or more prepare messages respectively from (Q-1) or more of the backup nodes, wherein Q (quorum) is $(N+F+1)/2$ rounded up to the nearest integer, and F is $(N-1)/3$ rounded down to the nearest integer;
- multicasting a commit message to at least some of the primary node and the other backup nodes, the commit message indicating that the one backup node agrees to the (Q-1) or more prepare messages; and
- obtaining, respectively from Q or more nodes among the primary node and the backup nodes, Q or more commit messages each indicating that the corresponding node agrees to (Q-1) or more prepare messages received by the corresponding node.

11. The method of claim 10, wherein:

before obtaining the pre-prepare message from the primary node, the method further comprises obtaining one or more transaction requests from at least one of: one or more clients, the primary node, or one or more of the other backup nodes; and

after obtaining the Q or more commit messages, the method further comprises packing the one or more transactions into a new block to add to a local copy of the blockchain.

12. The method of claim 10 or 11, wherein:

- the (Q-1) or more prepare messages include the multicast prepare message; and
- the Q or more commit messages include the multicast commit message.

13. A consensus system, comprising:

- one or more processors; and
- one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 12.

14. A consensus apparatus, comprising a plurality of modules for performing the method of any of claims 1 to 12.

15. A non-transitory computer-readable medium having stored therein instructions that, when executed by a processor of a device, cause the device to perform the method of any of claims 1 to 12.