

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 backup nodes, the method comprising:

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;

storing the pre-prepare message and the (Q-1) or more prepare messages;

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.

2. The method of claim 1, 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.

3. The method of claim 2, wherein:

the pre-prepare message comprises an order of one or more transactions corresponding to the one or more transaction requests; and

the commit message indicates that the corresponding node that sent the commit message agrees to the order.

4. The method of claim 3, further comprising:

packing the one or more transactions into a local copy of the blockchain maintained by the one backup node according to the order.

5. The method of any preceding claim, 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.

6. The method of any preceding claim, wherein storing the pre-prepare message and the (Q-1) or more prepare messages comprises:
storing only the pre-prepare message and the (Q-1) or more prepare messages.

7. The method of any preceding claim, after multicasting the commit message, further comprising:
performing a system restart; and
loading the stored pre-prepare message and the stored (Q-1) or more prepare messages.

8. The method of any of the claims 1-6, after storing the pre-prepare message and the (Q-1) or more prepare messages and before multicasting the commit message, further comprising:
performing a system restart; and
loading the stored pre-prepare message and the stored (Q-1) or more prepare messages.

9. The method of claim 8, after storing the pre-prepare message and the (Q-1) or more prepare messages and before multicasting the commit message, further comprising:
multicasting a view change message comprising the loaded pre-prepare message and the loaded (Q-1) or more prepare messages.

10. The method of claim 9, after storing the pre-prepare message and the (Q-1) or more prepare messages and before multicasting the commit message, further comprising:

obtaining from a new primary node a new view message indicating that the new primary node has received Q or more view change messages each indicating that the corresponding node agrees to the view change message;

multicasting another prepare message to at least some of the backup nodes including the new primary node, the another prepare message indicating an acceptance of the new view message; and

obtaining another (Q-1) or more prepare messages respectively from (Q-1) or more of the backup nodes.

11. The method of claim 10, wherein:

the Q or more view change messages include the multicast view change message; and

the another (Q-1) or more prepare messages include the another multicast prepare message.

12. The method of claim 9, after storing the pre-prepare message and the (Q-1) or more prepare messages and before multicasting the commit message, further comprising:

obtaining, respectively from Q or more of the backup nodes, Q or more view change messages each indicating that the corresponding node agrees to the view change message;

multicasting to at least some of the backup nodes a new view message indicating that the one backup node acting as a new primary node has received the Q or more view change messages; and

obtaining another (Q-1) or more prepare messages respectively from (Q-1) or more of the backup nodes.

13. The method of claim 8, wherein performing the system restart comprises:

performing the system restart without triggering a view change.

14. A consensus system acting as one of the backup nodes for maintaining the blockchain, 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 13.

15. A consensus apparatus acting as one of the backup nodes for maintaining the blockchain, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 13.