

CLAIMS:

1. A computer-implemented view change method to be implemented on a blockchain maintained by a number (N) of nodes, the method performed by a first node of the N nodes that is in a view change protocol, the method comprising:

obtaining, respectively from at least Q second nodes of the N nodes, at least Q first messages each comprising (1) a consistent current view known to the second node indicating a primary node designated among the N nodes and (2) a consistent current sequence number known to the second node, the current sequence number associated with a latest block or a latest transaction committed by the second node, wherein the current sequence number is larger than a first sequence number known to the first 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; and

responsive to obtaining the at least Q first messages, ending the view change protocol.

2. The method of claim 1, wherein obtaining the at least Q first messages comprises:

obtaining, respectively from the at least Q second nodes, at least Q commit messages indicating that the at least Q second nodes agree upon a next block to add to the blockchain, the Q commit messages respectively comprising the Q first messages.

3. The method of claim 1, wherein obtaining the at least Q first messages comprises:

obtaining, respectively from the at least Q second nodes, at least Q commit messages indicating that the at least Q second nodes agree upon a next block to add to the blockchain, the Q first messages respectively appended to the Q commit messages.

4. The method of any of claims 1-3, wherein:

the current sequence number comprises a height of a second copy of the blockchain maintained by the second node; and

the first sequence number comprises a height of a first copy of the blockchain maintained by the first node.

5. The method of any of claims 1-3, wherein:

the current sequence number comprises a sequence number of the latest transaction committed by the second node; and

the first sequence number comprises a sequence number of a latest transaction committed by the first node.

6. The method of any preceding claim, wherein:

the first message comprises a digital signature certifying the current view and the current sequence number both known to the second node.

7. The method of any preceding claim, wherein:

the first message further comprises a digest of the latest block or the latest transaction.

8. The method of claim 7, wherein:

the digest comprises a hash value of the latest block or the latest transaction.

9. The method of any of claims 7 and 8, wherein:

the digest comprises a Merkle root of the latest block known to the second node but unknown to the first node.

10. The method of any preceding claim, wherein ending the view change protocol comprises:

synchronizing a first copy of the blockchain maintained by the first node with a second copy of the blockchain maintained by the second node; and

exiting the view change protocol to enter a normal operation protocol using the consistent current view for the first node.

11. The method of any preceding claim, wherein:

the current sequence number known to the at least Q second nodes is (n+1);
and

the first sequence number known to the first node is n .

12. The method of any preceding claim, wherein:
the current view for the at least Q second nodes is v ; and
when in the view change protocol, the first node has a first view larger than v .

13. The method of any preceding claim, wherein:
the N nodes form a Practical Byzantine Fault Tolerance (PBFT) network, in which one of the N nodes acts as the primary node and the other $(N-1)$ nodes act as backup nodes.

14. A view change 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 13.

15. A view change apparatus, comprising a plurality of modules for performing the method of any of claims 1 to 13.