CLAIMS:

1. A computer-implemented consensus 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:

multicasting a view change message to at least some of the N nodes;

obtaining, respectively from at least Q second nodes of the N nodes, at least Q echo 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 largest 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 echo messages, ending the view change protocol.

2. The method of claim 1, wherein:

the at least Q echo messages are respectively sent by the at least Q second nodes to the first node in response to the at least Q second nodes obtaining the view change message.

3. The method of any of claims 1 and 2, wherein:

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

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

4. The method of any of claims 1 and 2, wherein:

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

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

5. The method of any preceding claim, wherein:

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

6. The method of any preceding claim, wherein:

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

7. The method of claim 6, wherein:

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

8. The method of any of claims 6 and 7, wherein:

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

9. 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 second node; and

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

10. The method of any preceding claim, wherein:

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

the largest sequence number known to the first node is n;

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.

11. 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.

12. 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 11.

13. A view change apparatus, comprising a plurality of modules for performing the method of any of claims 1 to 11.

14. A computer-implemented consensus method to be implemented on a blockchain maintained by a number (N) of nodes, the method performed by a second node of the N nodes that is in a normal operation protocol, the method comprising:

obtaining a view change message from a first node that is in a view change protocol;

determining a current protocol status of the second node; and

in response to determining that the current protocol status is the normal operation protocol, transmitting to the first node an echo message for the first node to exit the view change protocol based on receiving at least Q consistent echo messages from Q of the N nodes that are in the normal operation protocol, the echo message comprising (1) a current view known to the second node indicating a primary node designated among the N nodes and (2) a 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.

15. The method of claim 14, wherein:

the current sequence number is larger than a largest sequence number known to the first node.

16. The method of any of claims 14 and 15, wherein:

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

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

17. The method of any of claims 14 and 15, wherein:

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

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

18. The method of any of claims 14-17, wherein:

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

19. The method of any of claims 14-17, wherein:

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

20. The method of claim 19, wherein:

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

21. The method of any of claims 19 and 20, wherein:

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

22. The method of any of claims 14-21, wherein:

the current sequence number known to the second node is (n+1);

the largest sequence number known to the first node is n;

the current view for the second node is v; and

when in the view change protocol, the first node has a first view larger than v.

23. The method of any of claims 14-23, 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.

24. 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 14 to 23.

25. A view change apparatus, comprising a plurality of modules for performing the method of any of claims 14 to 23.