CLAIMS

What is claimed is:

1. A blockchain consensus method, comprising:

(i) performing, by a target consensus node of a blockchain, a current round of consensus, to count consensus votes of a number (N) of consensus proposals;

(ii) traversing, by the target consensus node, a first set of consensus proposals, to perform the following steps: migrating consensus proposals that each receive greater than or equal to f+1 and less than 2f+1 identical consensus votes into a second set of consensus proposals; and migrating consensus proposals that each receive less than f+1 identical consensus votes into a third set of consensus proposals as opposition consensus opinions, wherein f is a number of fault tolerant consensus nodes of the blockchain;

(iii) traversing, by the target consensus node, a fourth set of consensus proposals, to perform the following steps: migrating consensus proposals that each receive greater than or equal to 2f+1 identical consensus votes into the second set of consensus proposals; migrating consensus proposals that each receive greater than or equal to f+1 and less than 2f+1 identical consensus votes and are traceable based on an erasure coding algorithm into the second set of consensus proposals as agreement consensus opinions; migrating consensus proposals that each receive greater than or equal to f+1 and less than 2f+1 identical consensus votes and are untraceable based on the erasure coding algorithm into the third set of consensus proposals as opposition consensus opinions; and migrating consensus proposals that each receive less than f+1 identical consensus votes into the third set of consensus proposals as opposition consensus opinions, wherein the fourth set of consensus proposals stores the N consensus proposals in a first round of consensus, and the first set of consensus proposals is an absolute complement of the fourth set of consensus proposals for the N consensus proposals;

(iv) merging, by the target consensus node, the second set of consensus proposals into the first set of consensus proposals, and merging the third set of consensus proposals into the fourth set of consensus proposals, to perform a next round of consensus;

recursively performing, by the target consensus node, the steps (i)-(iv) until the first set of consensus proposals stores the N consensus proposals and the N consensus proposals each receive greater than or equal to 2f+1 identical consensus votes; and

determining, by the target consensus node, a consensus result based on counted consensus votes of the N consensus proposals in the last round of consensus.

2. The method according to claim 1, further comprising:

before the first round of consensus is performed, transmitting, by the target consensus node, based on an epoch message in a reliable broadcast (RBC) protocol, consensus proposals initiated by the target consensus node to other consensus nodes of the blockchain, and after receiving consensus proposals transmitted through epoch messages by 2f of the other consensus nodes of the blockchain, tracing, by the target consensus node based on the erasure coding algorithm, remaining consensus proposals not received; and

in the first round of consensus, casting, by the target consensus node, opposition consensus votes for consensus proposals that are untraceable based on the erasure coding algorithm in an RBC protocol stage and agreement consensus votes for remaining consensus proposals that are traceable based on the erasure coding algorithm in the RBC protocol stage.

3. The method according to claim 1, wherein:

the target consensus node traverses the fourth set of consensus proposals to further perform the following step: migrating consensus proposals that each receive only opposition

consensus votes into the second set of consensus proposals.

4. The method according to claim 1, further comprising:

exchanging, by the target consensus node, a Consensus Message respectively with other consensus nodes of the blockchain to count the consensus votes of the N consensus proposals, wherein the Consensus Message transmitted by the target consensus node comprises: a field value of consensus votes of consensus proposals in the fourth set of consensus proposals and a field value of consensus votes of consensus proposals in the first set of consensus proposals recorded by the target consensus node.

5. The method according to claim 4, wherein:

a field value of a consensus vote of a consensus proposal agreed by the target consensus node in the Consensus Message is a root hash corresponding to the consensus proposal, and a field value of a consensus vote of a consensus proposal opposed by the target consensus node in the Consensus Message is 0.

6. The method according to claim 4, wherein:

the Consensus Message further comprises: a field value indicating a serial number of a consensus view and/or a field value indicating a consensus round.

7. The method according to claim 4, further comprising:

after counting Consensus Messages transmitted by 2f other consensus nodes, traversing, by the target consensus node, the first set of consensus proposals.

8. The method according to claim 1, further comprising:

after completely traversing the first set of consensus proposals, determining, by the target consensus node, whether the first set of consensus proposals stores the N consensus proposals and whether the N consensus proposals each receive greater than or equal to 2f+1 identical consensus votes; and

if the first set of consensus proposals stores the N consensus proposals and the N consensus proposals each receive greater than or equal to 2f+1 identical consensus votes, ending, by the target consensus node, the consensus.

9. The method according to claim 1, wherein:

the N consensus proposals are initiated by different consensus nodes of the blockchain, any consensus proposal has one and only one type of consensus votes of a number greater than or equal to 2f+1, and a corresponding consensus result of any consensus proposal is a result indicated by the consensus votes of the number greater than or equal to 2f+1.

10. One or more non-transitory computer-readable storage media storing instructions executable by one or more processors, wherein execution of the instructions causes the one or more processors to perform operations comprising:

(i) performing a current round of consensus, to count consensus votes of a number (N) of consensus proposals;

(ii) traversing a first set of consensus proposals, to perform the following steps: migrating consensus proposals that each receive greater than or equal to f+1 and less than 2f+1 identical consensus votes into a second set of consensus proposals; and migrating consensus proposals that each receive less than f+1 identical consensus votes into a third set of consensus proposals as opposition consensus opinions, wherein f is a number of fault tolerant consensus nodes of a blockchain;

(iii) traversing a fourth set of consensus proposals, to perform the following steps: migrating consensus proposals that each receive greater than or equal to 2f+1 identical consensus votes into the second set of consensus proposals; migrating consensus proposals that each receive greater than or equal to f+1 and less than 2f+1 identical consensus votes and are traceable based on an erasure coding algorithm into the second set of consensus proposals as agreement consensus opinions; migrating consensus proposals that each receive greater than or equal to f+1 and less than 2f+1 identical consensus votes and are untraceable based on the erasure coding algorithm into the third set of consensus proposals as opposition consensus opinions; and migrating consensus proposals that each receive less than f+1 identical consensus votes into the third set of consensus proposals as opposition consensus opinions, wherein the fourth set of consensus proposals stores the N consensus proposals in a first round of consensus, and the first set of consensus proposals is an absolute complement of the fourth set of consensus proposals for the N consensus proposals;

(iv) merging the second set of consensus proposals into the first set of consensus proposals, and merging the third set of consensus proposals into the fourth set of consensus proposals, to perform a next round of consensus;

recursively performing the steps (i)-(iv) until the first set of consensus proposals stores the N consensus proposals and the N consensus proposals each receive greater than or equal to 2f+1 identical consensus votes; and

determining a consensus result based on counted consensus votes of the N consensus proposals in the last round of consensus.

11. The one or more non-transitory computer-readable storage media according to claim 10, wherein the operations further comprise:

before the first round of consensus is performed, transmitting based on an epoch message in a reliable broadcast (RBC) protocol, consensus proposals initiated by a target consensus node of the blockchain to other consensus nodes of the blockchain, and after receiving consensus proposals transmitted through epoch messages by 2f of the other consensus nodes of the blockchain, tracing, based on the erasure coding algorithm, remaining consensus proposals not received; and

in the first round of consensus, casting opposition consensus votes for consensus proposals that are untraceable based on the erasure coding algorithm in an RBC protocol stage and agreement consensus votes for remaining consensus proposals that are traceable based on the erasure coding algorithm in the RBC protocol stage.

12. The one or more non-transitory computer-readable storage media according to claim 10, wherein the operations further comprise:

traversing the fourth set of consensus proposals to perform the following step: migrating consensus proposals that each receive only opposition consensus votes into the second set of consensus proposals.

13. The one or more non-transitory computer-readable storage media according to claim 10, wherein the operations further comprise:

exchanging a Consensus Message respectively with other consensus nodes of the blockchain to count the consensus votes of the N consensus proposals, wherein the Consensus Message comprises: a field value of consensus votes of consensus proposals in the fourth set of consensus proposals and a field value of consensus votes of consensus proposals in the first set of consensus proposals.

14. The one or more non-transitory computer-readable storage media according to claim

13, wherein:

a field value of a consensus vote of a consensus proposal agreed to in the Consensus Message is a root hash corresponding to the consensus proposal, and a field value of a consensus vote of a consensus proposal opposed to in the Consensus Message is 0.

15. The one or more non-transitory computer-readable storage media according to claim 13, wherein:

the Consensus Message further comprises: a field value indicating a serial number of a consensus view and/or a field value indicating a consensus round.

16. The one or more non-transitory computer-readable storage media according to claim 13, wherein the operations further comprise:

after counting Consensus Messages transmitted by 2f other consensus nodes, traversing the first set of consensus proposals.

17. The one or more non-transitory computer-readable storage media according to claim 10, wherein the operations further comprise:

after completely traversing the first set of consensus proposals, determining whether the first set of consensus proposals stores the N consensus proposals and whether the N consensus proposals each receive greater than or equal to 2f+1 identical consensus votes; and

if the first set of consensus proposals stores the N consensus proposals and the N consensus proposals each receive greater than or equal to 2f+1 identical consensus votes, ending the consensus.

18. The one or more non-transitory computer-readable storage media according to claim 10, wherein:

the N consensus proposals are initiated by different consensus nodes of the blockchain, any consensus proposal has one and only one type of consensus votes of a number greater than or equal to 2f+1, and a corresponding consensus result of any consensus proposal is a result indicated by the consensus votes of the number greater than or equal to 2f+1.

19. A system comprising one or more processors and one or more non-transitory computer-readable memories coupled to the one or more processors and configured with instructions executable by the one or more processors to cause the system to perform operations comprising:

(i) performing a current round of consensus, to count consensus votes of a number (N) of consensus proposals;

(ii) traversing a first set of consensus proposals, to perform the following steps: migrating consensus proposals that each receive greater than or equal to f+1 and less than 2f+1 identical consensus votes into a second set of consensus proposals; and migrating consensus proposals that each receive less than f+1 identical consensus votes into a third set of consensus proposals as opposition consensus opinions, wherein f is a number of fault tolerant consensus nodes of a blockchain;

(iii) traversing a fourth set of consensus proposals, to perform the following steps: migrating consensus proposals that each receive greater than or equal to 2f+1 identical consensus votes into the second set of consensus proposals; migrating consensus proposals that each receive greater than or equal to f+1 and less than 2f+1 identical consensus votes and are traceable based on an erasure coding algorithm into the second set of consensus proposals as agreement consensus opinions; migrating consensus proposals that each receive greater than or equal to f+1 and less than 2f+1 identical consensus votes and are untraceable based on the

erasure coding algorithm into the third set of consensus proposals as opposition consensus opinions; and migrating consensus proposals that each receive less than f+1 identical consensus votes into the third set of consensus proposals as opposition consensus opinions, wherein the fourth set of consensus proposals stores the N consensus proposals in a first round of consensus, and the first set of consensus proposals is an absolute complement of the fourth set of consensus proposals for the N consensus proposals;

(iv) merging the second set of consensus proposals into the first set of consensus proposals, and merging the third set of consensus proposals into the fourth set of consensus proposals, to perform a next round of consensus;

recursively performing the steps (i)-(iv) until the first set of consensus proposals stores the N consensus proposals and the N consensus proposals each receive greater than or equal to 2f+1 identical consensus votes; and

determining a consensus result based on counted consensus votes of the N consensus proposals in the last round of consensus.

20. The system of claim 19, wherein the operations further comprise:

before the first round of consensus is performed, transmitting based on an epoch message in a reliable broadcast (RBC) protocol, consensus proposals initiated by a target consensus node of the blockchain to other consensus nodes of the blockchain, and after receiving consensus proposals transmitted through epoch messages by 2f of the other consensus nodes of the blockchain, tracing, based on the erasure coding algorithm, remaining consensus proposals not received; and

in the first round of consensus, casting opposition consensus votes for consensus proposals that are untraceable based on the erasure coding algorithm in an RBC protocol stage and agreement consensus votes for remaining consensus proposals that are traceable based on the erasure coding algorithm in the RBC protocol stage.