CLAIMS

What is claimed is:

1. A consensus method in a consortium blockchain, comprising:

broadcasting, by a first consensus node, a ViewChange message in a consensus network based on received ECHO messages broadcast for target consensus data and received signatures when the first consensus node in the consensus network of the consortium blockchain does not complete a consensus operation on the target consensus data within a predetermined time period, wherein the ECHO messages broadcast for the target consensus data and the signatures are sent by other consensus nodes in the consensus network, and wherein the ECHO messages comprise uncompleted PRE-PREPARE and PREPARE messages;

receiving, by a first consensus primary node in the consensus network, the ViewChange message broadcast by a first consensus node in the consensus network, wherein the first consensus primary node is an updated consensus primary node after the view change determined based on the ViewChange message;

constructing, by the first consensus primary node, a NewView message including ECHO messages and signatures in N−f verified ViewChange messages as prepared data P when the first consensus primary node determines that the N−f verified ViewChange messages are received; adding all valid prepared data P to the ECHO messages comprising the uncompleted PRE-PREPARE and PREPARE messages, and broadcasting the constructed NewView message to the consensus network to change a view of the consensus network to a target view, wherein f is a maximum quantity of abnormal consensus nodes allowed in the consensus network, N is a quantity of consensus nodes in the consensus network, and $N \geq 3f+1$; and

broadcasting, by a second consensus node, the ECHO message for the target consensus data in the consensus network when the second consensus node that receives the NewView message determines that the present consensus node has an ECHO message corresponding to the target consensus data, wherein a view number in the ECHO message is a view number of the target view.

2. The method according to claim 1, wherein before the broadcasting, by a first consensus node, a ViewChange message in a consensus network, the method further comprises:

splitting, by the second consensus primary node in the consensus network based on a specified erasure coding technology, the target consensus data into a plurality of orderly arranged data fragments that have a same quantity as the consensus nodes in the consensus network, wherein the second consensus primary node is a consensus primary node corresponding to a previous view of a view corresponding to the first consensus primary node;

constructing, by the second consensus primary node, a Merkle tree based on the plurality of orderly arranged data fragments; and

locally saving, by the second consensus primary node, a data fragment corresponding to the second consensus primary node, a corresponding Merkle tree path, and a root hash of the Merkle tree, and sending, to corresponding consensus nodes in the consensus network, VAL messages comprising other data fragments, corresponding Merkle tree paths, and the root hash of the Merkle tree, wherein one data fragment corresponds to one consensus node in the consensus network.

3. The method according to claim 2, wherein after the locally saving, by the second consensus primary node, a data fragment corresponding to the second consensus primary node, a corresponding Merkle tree path, and a root hash of the Merkle tree, and sending, to corresponding consensus nodes in the consensus network, VAL messages comprising other data fragments, corresponding Merkle tree paths, and the root hash of the Merkle tree, the method further comprises:

constructing, by a third consensus node that receives a VAL message, an ECHO message for the received VAL message, and broadcasting the constructed ECHO message to the consensus network, wherein the constructed ECHO message comprises a data fragment, a corresponding Merkle tree path, and the root hash of the Merkle tree in the received VAL message; and

constructing, by the second consensus primary node, an ECHO message based on the locally saved data fragment, corresponding Merkle tree path, and root hash of the Merkle tree, and broadcasting the constructed ECHO message to the consensus network.

4. The method according to claim 3, wherein the constructing, by the first consensus primary node, a NewView message including ECHO messages and signatures in N−f verified ViewChange messages as prepared data when the first consensus primary node determines that the N−f verified ViewChange messages are received comprises:

determining, by the first consensus primary node, whether a hash value of an ECHO message in each of the received ViewChange messages is consistent with data obtained by decrypting a signature corresponding to the ECHO message by using a public key;

when hash values of N−f ECHO messages in the ECHO messages in the received ViewChange messages are consistent with data obtained by decrypting signatures corresponding to the ECHO messages, determining, by the first consensus primary node, that the N−f verified ViewChange messages are received; and

constructing, by the first consensus primary node, the NewView message based on the ECHO messages and the signatures in the N−f verified ViewChange messages.

5. The method according to claim 4, wherein the constructing, by the first consensus primary node, a NewView message including ECHO messages and signatures in N−f verified ViewChange messages as prepared data P comprises:

obtaining, by the first consensus primary node, corresponding N−f data fragments based on the ECHO messages and the signatures in the N−f verified ViewChange messages;

constructing, by the first consensus primary node, the Merkle tree based on the N−f data fragments, and obtaining the root hash of the Merkle tree; and

constructing, by the first consensus primary node, the NewView message based on the root hash of the Merkle tree, the N−f verified ViewChange messages, and a block number corresponding to the target consensus data.

6. The method according to claim 5, wherein the broadcasting, by a second consensus node, the ECHO message for the target consensus data in the consensus network when the second consensus node that receives the NewView message determines that the present consensus node has an ECHO message corresponding to the target consensus data comprising:

broadcasting the ECHO message for the target consensus data in the consensus network when the second consensus node that receives the NewView message determines that the present consensus node has an ECHO message comprising the root hash of the Merkle tree.

7. The method according to claim 6, wherein the broadcasting, by a second consensus node, the ECHO message for the target consensus data in the consensus network when the second consensus node that receives the NewView message

determines that the present consensus node has an ECHO message corresponding to the target consensus data comprising:

when the second consensus node that receives the NewView message determines that the present consensus node has the ECHO message corresponding to the target consensus data, constructing the ECHO message for the target consensus data based on a target data fragment in the ECHO message corresponding to the target consensus data in the present consensus node, a Merkle tree path of the target data fragment in the Merkle tree, the root hash of the Merkle tree, a view number obtained after view change, and the block number corresponding to the target consensus data; and

broadcasting, by the second consensus node that receives the NewView message, the ECHO message for the target consensus data in the consensus network after the view change.

8. The method according to claim 1, after the broadcasting, by the second consensus node that receives the NewView message, the ECHO message for the target consensus data in the consensus network after the view change, the method further comprises:

committing, by a fourth consensus node that receives the ECHO message for the target consensus data, the target consensus data to a state machine if the fourth consensus node receives ECHO messages of N−f consensus nodes for the target consensus data.

9. The method according to any one of claims 1 to 8, wherein

the first consensus node is any one of the consensus nodes in the consensus network, and the second consensus node is any one of the consensus nodes in the consensus network.

10. A system in a consortium blockchain, comprising:

a first consensus node, configured to: when the first consensus node does not complete a consensus operation on target consensus data within a predetermined time period, broadcast a ViewChange message in a consensus network based on ECHO messages broadcast for target consensus data and signatures that are received from other consensus nodes in the consensus network of the consortium blockchain, wherein the ECHO messages comprise uncompleted PRE-PREPARE and PREPARE messages;

a consensus primary node, configured to receive the ViewChange message broadcast by the first consensus node in the consensus network, wherein the

consensus primary node is an updated consensus primary node after the view change determined based on the ViewChange message; and construct a NewView message including ECHO messages and signatures in N−f verified ViewChange messages as prepared data P when the consensus primary node determines that the N−f verified ViewChange messages are received, add all valid prepared data P to the ECHO messages comprising the uncompleted PRE-PREPARE and PREPARE messages, and broadcast the constructed NewView message to the consensus network to change a view of the consensus network to a target view, wherein f is a maximum quantity of abnormal consensus nodes allowed in the consensus network, N is a quantity of consensus nodes in the consensus network, and $N \geq 3f+1$; and

a second consensus node, configured to broadcast the ECHO message for the target consensus data in the consensus network when the second consensus node that receives the NewView message determines that the present consensus node has an ECHO message corresponding to the target consensus data, wherein a view number in the ECHO message is a view number of the target view.