

CLAIMS

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

when a target consensus node of a consortium blockchain performs a consensus operation on
5 a target consensus proposal, sending a verification signature to another consensus node of the
consortium blockchain, wherein the verification signature is used to represent at least one
consensus verification item set by the consensus node sending the verification signature itself for
the target consensus proposal, and wherein at least part of consensus nodes in the consortium
blockchain set a consensus verification item that is configured to perform risk verification
10 according to their own security data;

receiving, by the target consensus node, a verification signature sent by another consensus
node of the consortium blockchain for the target consensus proposal; and

after the target consensus node reaches a consensus on proposal data of the target consensus,
generating a block recording a collected verification signature corresponding to the target
15 consensus and the proposal data, wherein the verification signature recorded in the block is used
to prove the validity of the proposal data recorded in the block.

2. The method according to claim 1, wherein

the consensus nodes of the consortium blockchain perform the target consensus based on a
Practical Byzantine Fault Tolerance (PBFT) protocol; and

20 sending, by the target consensus node, a verification signature to another consensus node of
the consortium blockchain after a consensus operation is performed on a target consensus proposal
comprises:

sending, by the target consensus node, a verification signature to another consensus node of
the consortium blockchain through a commit message at a commit stage of the PBFT protocol.

25 3. The method according to claim 1, wherein

the consensus nodes of the consortium blockchain perform the target consensus based on a HoneyBadger Byzantine Fault Tolerance (HoneyBadgerBFT) protocol; and

sending, by the target consensus node, a verification signature to another consensus node of the consortium blockchain after a consensus operation is performed on a target consensus proposal

5 comprises:

sending, by the target consensus node, a verification signature to another consensus node of the consortium blockchain based on a signature message after an ACS stage of the HoneyBadgerBFT protocol ends.

4. The method according to claim 1, wherein

10 different consensus nodes in the consortium blockchain are provided with the same or at least partially different consensus verification items.

5. The method according to claim 1, wherein

a consensus verification item set by at least part of consensus nodes in the consortium blockchain comprises at least one of the following:

15 verification on a hash value of a local last block, verification on a timestamp of the target consensus, and verification on proposal data of the target consensus.

6. A data verification method of a consortium blockchain, comprising:

extracting, from a target block of a target consensus node of a consortium blockchain, recorded proposal data and a verification signature from at least one consensus node in the consortium blockchain, wherein the proposal data in the target block comes from a target consensus proposal, and the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal.

and wherein at least part of consensus nodes in the consortium blockchain set a consensus verification item that is configured to perform risk verification according to their own security data;

25 and

verifying the validity of the proposal data recorded in the target block based on a quantity of verification signatures extracted from the target block.

7. The method according to claim 6, wherein

verifying the proposal data recorded in the target block based on the quantity of the verification signatures extracted from the target block comprises:

if the quantity of the verification signatures extracted from the target block reaches $2F+1$, determining that the proposal data recorded in the target block succeeds in the validity verification, wherein F is a quantity of abnormal consensus nodes tolerable by the consortium blockchain.

8. A consensus node of a consortium blockchain, wherein at least part of consensus nodes in the consortium blockchain set a consensus verification item that is configured to perform risk verification according to their own security data, wherein the consensus node comprises:

a sending module configured to, when a consensus operation is performed on a target consensus proposal, send a verification signature to another consensus node of the consortium blockchain, wherein the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal;

a receiving module configured to receive a verification signature sent by another consensus node of the consortium blockchain for the target consensus proposal; and

a block generation module configured to, after a consensus is reached on proposal data of the target consensus, generate a block recording a collected verification signature corresponding to the target consensus and the proposal data, wherein the verification signature recorded in the block is used to prove the validity of the proposal data recorded in the block.

9. A consortium blockchain system, comprising a plurality of consensus nodes, wherein a target consensus node among the plurality of consensus nodes performs the following when participating in a target consensus:

sending a verification signature to another consensus node of the consortium blockchain, wherein the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal,

and wherein at least part of consensus nodes in the consortium blockchain set a consensus verification item that is configured to perform risk verification according to their own security data;

receiving a verification signature sent by another consensus node of the consortium blockchain for the target consensus proposal; and

after a consensus is reached on proposal data of the target consensus, generating a block recording a collected verification signature corresponding to the target consensus and the proposal data, wherein the verification signature recorded in the block is used to prove the validity of the proposal data recorded in the block.

10. A data verification apparatus of a consortium blockchain, comprising:

an extraction module configured to extract, from a target block of a target consensus node of a consortium blockchain, recorded proposal data and a verification signature from at least one consensus node in the consortium blockchain, wherein the proposal data in the target block comes from a target consensus proposal, and the verification signature is used to represent at least one consensus verification item set by the consensus node sending the verification signature itself for the target consensus proposal, and wherein at least part of consensus nodes in the consortium blockchain set a consensus verification item that is configured to perform risk verification according to their own security data; and

a verification module configured to verify the validity of the proposal data recorded in the target block based on a quantity of verification signatures extracted from the target block.