

CLAIMS

1. A business verification method, comprising:

receiving, by a first block chain node in a whole consensus network, a business request sent by a terminal;

5 storing, at the first block chain node, the business request in a business memory corresponding to the first block chain node, and broadcasting the business request to second block chain nodes in the whole consensus network;

receiving, at some second block chain nodes, the business request broadcast by the first block chain node, wherein at least one of the second block chain nodes in the whole consensus network does not receive the business request broadcast by the first
10 block chain node due to a network failure between the at least one of the second block chain nodes and the first block chain node;

storing the business request in respective corresponding business memories of the second block chain nodes;

15 gaining, at the first block chain node, at least one business request from the business memory of the first block chain node;

packaging, at the first block chain node, the gained at least one business request into a pre-processed block and broadcasting the pre-processed block of the at least one business request to the second block chain nodes for consensus verification;

20 receiving, by the second block chain nodes, the pre-processed block of the at least one business request;

carrying out consensus verification, at the second block chain nodes on the pre-processed block of the at least one business request according to business requests included in respective corresponding business memories and matching with the at least
25 one business request from the business memory of the first block chain node;

in response to a second block chain node finding that a business memory corresponding thereto does not include a part of the at least one business request in the pre-processed block, wherein the second block chain node does not receive the part of the at least one business request due to the network failure, determining, by the second
30 block chain node, that the pre-processed block of the at least one business request in local consensus verification is not directly failed;

acquiring, by the second block chain node, the part of the at least one business

request that is not included in the business memory corresponding thereto from other block chain nodes in the whole consensus network; and

carrying out consensus verification, at the second block chain node on the at least one business request included in the pre-processed block by using the acquired
5 part of the at least one business request and business requests stored in the business memory of the second block chain node.

2. The method of claim 1, wherein the business memories of the first block chain node and the second block chain nodes are set in form of a database that stores business requests, and wherein the business requests stored in a business
10 memory do not disappear in case of failure of a corresponding block chain node.

3. The method of claim 2, wherein the step of storing the business request in the business memory corresponding to the first block chain node specifically comprises:

sending the business request sent from the terminal to a preset distributed
15 middleware for data transmission between the block chain nodes and the business memories in the whole consensus network; and

storing the business request in the business memory corresponding to the first block chain node, according to a node identifier of the first block chain node, by using a preset distributed middleware.

20 4. The method of any one of claims 1 to 3, wherein the step of gaining at least one business request from the business memory specifically comprises:

gaining, from the business memory, a set number of business requests with a business type higher than a set priority.

5. The method of claim 4, wherein the step of storing the business request
25 in a business memory corresponding to the first block chain node specifically comprises:

ranking, by the first block chain node, the business request and previously received business requests according to a preset priority sequence of business types.

6. The method of claim 1, wherein the first block chain node is a leader
30 node in a consortium chain consensus algorithm, and the second block chain node is a non-leader node in the consortium chain consensus algorithm.

7. The method of claim 1, wherein the step of acquiring, by the second block chain node, the part of the at least one business request that is not included in the business memory corresponding thereto from the other block chain nodes in the whole consensus network comprises:
- 5 sending a query message for acquiring the part of the at least one business request to another second block chain node or the first block chain node when it is determined that the business memory of the second block chain node does not comprise the part of the at least one business request in the pre-processed block;
- 10 receiving a reply message returned by the another second block chain node or the first block chain node, the reply message indicating that a business memory corresponding to the another second block chain node or the first block chain node sending the reply message stores the part of the at least one business request; and
- 15 acquiring the part of the at least one business request from the business memory corresponding to the second block chain node or the first block chain node sending the reply message.
8. The method of claim 1, further comprising:
- after receiving the business request sent by the first block chain node, the second block chain node further broadcasting the business request to other block chain nodes in the whole consensus network;
- 20 at the other block chain nodes when receiving the business request, judging whether the business request has been previously received;
- if yes, the other block chain nodes ignore the business request; and
- if no, the other block chain nodes store the business request in business memories corresponding thereto by using a preset distributed middleware.
- 25 9. The method of claim 8, further comprising:
- during the consensus verification, after receiving the pre-processed block, verifying, by the second block chain nodes, legality of asymmetric signatures of the business requests included in the pre-processed block.
10. The method of claim 9, further comprising:
- 30 according to the asymmetric signature legality verification and a Hash integrity verification carried out for the pre-processed block, obtaining by each of the block chain nodes a verification result of its own about whether the pre-processed block as a

whole is legal;

broadcasting, by each of the block chain nodes, the verification result obtained by itself to other block chain nodes; and

5 according to verification results sent by the other block chain nodes for the pre-processed block and the verification result obtained by itself, each of the block chain nodes, obtaining an integrated verification result, about whether the pre-processed block passes the verifications, of the block chain nodes in the whole consensus network,

10 further broadcasting the obtained integrated verification result to the other block chain nodes;

after receiving the integrated verification results broadcast to each other, judging, by each of the block chain nodes in the consensus network, whether most of the integrated verification results obtained by the block chain nodes in the consensus network indicate that the verification is successful;

15 if yes, storing the business requests in the pre-processed block in a block chain of its own as blocks; and

if no, refusing the business requests in the pre-processed block.

11. A business verification apparatus comprising a plurality of modules configured to perform the method of any one of the claims 1 to 10.

20