

CONSENSUS METHODS AND SYSTEMS IN CONSORTIUM BLOCKCHAIN

TECHNICAL FIELD

[0001] The present specification relates to the field of computer technologies, and
5 in particular, to consensus methods and systems in a consortium blockchain.

BACKGROUND

[0002] At present, the practical Byzantine fault tolerance (PBFT) mainly includes two parts: a normal case phase and a view change phase. The normal case phase includes PRE-PREPARE, PREPARE, and COMMIT stages to complete a consensus.

10 [0003] In the PRE-PREPARE stage, a consensus primary node initiates a proposal, and sends a PRE-PREPARE message for the proposal to each consensus backup node. In the PREPARE stage, each consensus backup node verifies a received PRE-PREPARE message, and after the verification succeeds, sends a PREPARE message to other consensus backup nodes and the consensus primary node. In the COMMIT
15 stage, a consensus backup node or the consensus primary node receives one PRE-PREPARE message and PREPARE messages from not less than $2f$ consensus nodes, and sends a COMMIT message to other consensus nodes in the consortium blockchain if the verification succeeds.

[0004] However, if a consensus operation for the target proposal is not completed
20 within a predetermined time period, the consensus node in the consensus network can trigger a view change operation to attempt to replace the consensus primary node. In addition, in the process, consensus nodes other than the consensus primary node do not receive the PRE-PREPARE message that can be used to recover the original target proposal, where a failure already occurs in the primary node, the other consensus
25 nodes cannot recover the original target proposal. Consequently, the consensus operation on the target proposal cannot continue after view change.

SUMMARY

[0005] Embodiments of the present specification provide consensus methods and systems in a consortium blockchain to deal with a problem that, after a view change operation is performed in a round of consensus operation based on an existing PBFT consensus algorithm, continue to perform consensus of data that hasn't yet reached consensus can't be ensured.

[0006] To deal with the previous technical problem, some embodiments of the present specification are implemented as described below:

[0007] According to a first aspect, a consensus method in a consortium blockchain is provided, including:

[0008] When a first consensus node in a consensus network of the consortium blockchain does not complete a consensus operation on target consensus data within a predetermined time period, the first consensus node broadcasts a ViewChange message in the consensus network based on received ECHO messages broadcast for the target consensus data and received signatures, where the ECHO messages broadcast for the target consensus data and the signatures are sent by other consensus nodes in the consensus network.

[0009] The first consensus primary node in the consensus network receives the ViewChange message broadcast by a consensus node in the consensus network, where the first consensus primary node is a consensus primary node corresponding to a view existing when the consensus operation is performed on the target consensus data.

[0010] When the first consensus primary node determines that $N-f$ verified ViewChange messages are received, the first consensus primary node constructs a NewView message based on ECHO messages and signatures in the $N-f$ verified ViewChange messages, and broadcasts the constructed NewView message to the consensus network to change the view of the consensus network to a target view, where 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 $N \geq 3f+1$.

[0011] When a second consensus node that receives the NewView message determines that the present consensus node has an ECHO message corresponding to the target consensus data, the second consensus node broadcasts the ECHO message

for the target consensus data in the consensus network, where a view number in the ECHO message is a view number of the target view.

[0012] According to a second aspect, a system in a consortium blockchain is provided, including: 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; a consensus primary node, configured to receive the ViewChange message broadcast by the consensus node in the consensus network; and construct a NewView message based on ECHO messages and signatures in $N-f$ verified ViewChange messages when the consensus primary node determines that the $N-f$ verified ViewChange messages are received, and broadcast the constructed NewView message to the consensus network to change a view of the consensus network to a target view, where 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, where a view number in the ECHO message is a view number of the target view.

[0013] The embodiments of the present specification can achieve at least the following technical effects by using the previous technical solutions:

[0014] In the consensus method provided in the embodiments of the present specification, when the first consensus node in the consensus network of the consortium blockchain does not complete the consensus operation on the target consensus data within the predetermined time period, the first consensus node can broadcast the ViewChange message in the consensus network based on the ECHO messages broadcast for the target consensus data and the signatures that are sent by other consensus nodes in the consortium blockchain. The first consensus primary node in the consensus network receives the ViewChange message broadcast by the consensus node in the consensus network. When the first consensus primary node determines that the $N-f$ verified ViewChange messages are received, the first consensus primary node constructs the NewView message based on the ECHO

messages and the signatures in the N-f verified ViewChange messages, and broadcasts the constructed NewView message to the consensus network. 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, the second consensus node can broadcast the ECHO message for the target consensus data in the consensus network.

[0015] In other words, after a consensus node in the consensus network triggers a view change operation, any consensus node in the consensus network, i.e. the first consensus node, can broadcast the ViewChange message in the consensus network, and the ViewChange message includes the ECHO messages broadcast by the consensus nodes in the consortium blockchain for the target consensus data and the corresponding signatures that are received by the first consensus node. As such, even if the consensus node triggering the view change is not a consensus primary node after the view change, an ECHO message constructed by the consensus node in the consensus network for the target consensus data and a corresponding signature can still be obtained by other consensus nodes in the consensus network, so that the consensus node in the consensus network continues to perform the consensus operation on the target consensus data in the consensus network after the view change.

BRIEF DESCRIPTION OF DRAWINGS

[0016] The accompanying drawings described here are used to provide further understanding of the present specification, and constitute a part of the present specification. The example embodiments of the present specification and descriptions thereof are used to explain the present specification, and are not intended to constitute an undue limitation of the present specification. In the accompanying drawings:

[0017] FIG. 1 is a schematic flowchart illustrating view change in existing PBFT;

[0018] FIG. 2 is a schematic flowchart illustrating implementation of a consensus method in a consortium blockchain, according to some embodiments of the present specification;

[0019] FIG. 3 is a schematic diagram illustrating an actual scenario to which a consensus method in a consortium blockchain is applied, according to some embodiments of the present specification; and

[0020] FIG. 4 is a schematic structural diagram illustrating a system in a consortium blockchain, according to some embodiments of the present specification.

DESCRIPTION OF EMBODIMENTS

[0021] To make the objectives, technical solutions, and advantages of the present specification clearer, the following clearly and comprehensively describes the technical solutions of the present specification with reference to specific embodiments and accompanying drawings of the present specification. Clearly, the described embodiments are merely some but not all of the embodiments of the present specification. All other embodiments obtained by a person of ordinary skill in the art based on the embodiments of the present specification without creative efforts shall fall within the protection scope of the present specification.

[0022] The technical solutions provided in some embodiments of the present specification are described in detail below with reference to the accompanying drawings.

[0023] FIG. 1 is a schematic flowchart illustrating view change in existing PBFT algorithm. A consensus network shown in FIG. 1 includes four consensus nodes p0, p1, p2, and p3. p0 is a consensus primary node before the view change, and p3 is an abnormal consensus node in the consensus network.

[0024] In FIG. 1, if consensus primary node p0 works maliciously, consensus primary node p0 may assign a same sequence number to different requests, or does not assign a sequence number, or makes adjacent sequence numbers discontinuous. Consensus backup nodes (p1 to p3) in the consensus network should be responsible to proactively check validity of these sequence numbers. A view change in the consensus network can be triggered if consensus primary node p0 is offline or works maliciously and does not broadcast a request of a client device, then a consensus on data requested by the client device is not completed within a predetermined time period, i.e. a consensus backup node (any one of consensus node p1 to consensus node p3) detects that consensus primary node (p0) is offline or works maliciously due to timeout. A specific process can include the following:

[0025] The consensus backup node broadcasts a ViewChange message in the format of a message <VIEW-CHANGE, v+1, n, C, P, i> to other consensus nodes, where n is a newest stable checkpoint number, i.e. a block number corresponding to

data on which a consensus operation is performed currently, C is a set of $2f+1$ verified CheckPoint messages, and P is a set of requested PRE-PREPARE and PREPARE messages that are currently not completed by the consensus backup node.

[0026] When a new consensus primary node $p=v+1 \bmod |R|$ receives $2f$ valid

5 ViewChange messages after the view change, the new consensus primary node can broadcast a message $\langle \text{NEW-VIEW}, v+1, V, O \rangle$ to the other consensus nodes, where V is a set of valid ViewChange messages, and O is a set of uncompleted PRE-PREPARE messages that are re-initiated by the consensus primary node. A selection rule of a set of PRE-PREPARE messages is as follows:

10 **[0027]** 1. A minimum stable checkpoint number min-s in V and a maximum number max-s of a prepare message in V are selected.

[0028] 2. For min-s and max-s , if message set P exists, a message $\langle \langle \text{PRE-PREPARE}, v+1, n, d \rangle, m \rangle$ is created. Otherwise, an empty PRE-PREPARE message is created, i.e. $\langle \langle \text{PRE-PREPARE}, v+1, n, d(\text{null}) \rangle, m(\text{null}) \rangle$, $m(\text{null})$ is a null
15 message, and $d(\text{null})$ is a null message digest.

[0029] When receiving a NewView message of the new consensus primary node after the view change, the consensus backup node verifies the validity, and when the verification succeeds, enters a new view state after the view change, i.e. the new view state with a view number $v+1$, and starts processing the PRE-PREPARE message in
20 O .

[0030] In the consensus method provided in the embodiments of the present specification, when the first consensus node in the consensus network of the consortium blockchain does not complete the consensus operation on the target consensus data within the predetermined time period, the first consensus node can
25 broadcast the ViewChange message in the consensus network based on the ECHO messages broadcast for the target consensus data and the signatures that are sent by other consensus nodes in the consortium blockchain. A first consensus primary node in the consensus network receives the ViewChange message broadcast by a consensus node in the consensus network. When the first consensus primary node determines
30 that the $N-f$ verified ViewChange messages are received, the first consensus primary node constructs the NewView message based on the ECHO messages and the signatures in the $N-f$ verified ViewChange messages, and broadcasts the constructed NewView message to the consensus network. 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, the second consensus node can broadcast the ECHO message for the target consensus data in the consensus network.

5 **[0031]** In other words, after a consensus node in the consensus network triggers a view change operation, any consensus node in the consensus network, i.e. the first consensus node, can broadcast the ViewChange message in the consensus network, and the ViewChange message includes the ECHO messages broadcast by the consensus nodes in the consortium blockchain for the target consensus data and the corresponding signatures that are received by the first consensus node. As such, even
10 if the consensus node triggering the view change is not a consensus primary node after the view change, an ECHO message constructed by the consensus node in the consensus network for the target consensus data and a corresponding signature can still be obtained by other consensus nodes in the consensus network, so that the consensus node in the consensus network continues to perform the consensus
15 operation on the target consensus data in the consensus network after the view change.

[0032] Specifically, FIG. 2 is a schematic flowchart illustrating implementation of a consensus method in a consortium blockchain, according to one or more embodiments of the present specification. The method includes the following:

20 **[0033]** Step 210. When a first consensus node in a consensus network of the consortium blockchain does not complete a consensus operation on target consensus data within a predetermined time period, the first consensus node broadcasts a ViewChange message in the consensus network based on received ECHO messages broadcast for the target consensus data and received signatures, where the ECHO
25 messages broadcast for the target consensus data and the signatures are sent by other consensus nodes in the consensus network.

[0034] The format of the ViewChange message is ViewChange ($v+1$, n , C , P , i), where $v+1$ is a view number after view change, n is a block number corresponding to the target consensus data, C is a set of $N-f$ verified CheckPoint messages, P is
30 prepared data and includes $N-f$ ECHO messages with valid signatures, and the $N-f$ ECHO messages with the valid signatures are constructed by $N-f$ consensus nodes in the consensus network based on received VAL messages. N is a positive integer greater than or equal to $3f+1$, f is a maximum quantity of abnormal consensus nodes allowed in the consensus network, and when a state of the consensus node is changed

to a prepared state, it indicates that the consensus node has received the N-f ECHO messages with the valid signatures.

[0035] The first consensus node can be any consensus node in the consensus network, that is, the first consensus node can be any consensus backup node in the consortium blockchain, or a first consensus primary node, or a second consensus primary node. That is, any consensus node in the consensus network including the consensus primary node or the consensus backup node can trigger a view change operation in the consensus network when the consensus node does not complete the consensus operation on the target consensus data within the predetermined time period, to attempt to replace the consensus primary node in the consensus network.

[0036] It can be understood that the ViewChange message can include the ECHO messages broadcast by all consensus nodes in the consensus network for the target consensus data and the corresponding signatures that are received by the first consensus node. Specifically, the ECHO message can be constructed by the consensus node in the consensus network for the received VAL message in the normal case phase of a PBFT consensus algorithm. The ECHO message can include the block number corresponding to the target consensus data, current view number of the target consensus data, and original target consensus data. Specifically, the signature of the ECHO message can be a signature of the ECHO message that is obtained by each consensus node in the consensus network by using a private key of the consensus node.

[0037] When the target consensus data can be split, based on a specified erasure coding technology, into a plurality of data fragments that have a same quantity as the consensus nodes in the consensus network, the plurality of data fragments can be sent to corresponding consensus nodes in the consensus network by using VAL messages. Data fragments in the VAL messages received by the consensus nodes are different, and one data fragment corresponds to one consensus node in the consensus network. In this case, the ECHO message broadcast by the consensus node in the consensus network can specifically include the block number corresponding to the target consensus data, the number of the view showing the target consensus data currently, a data fragment corresponding to the consensus node, a Merkle tree path of the data fragment in a Merkle tree constructed by using the plurality of data fragments, and a root hash of the Merkle tree constructed by using the plurality of data fragments.

[0038] Optionally, to reduce network transmission bandwidth consumed by the consensus primary node in the consensus operation process, the target consensus data in some embodiments of the present specification can be split into the plurality of data fragments based on the specified erasure coding technology. Specifically, before the first consensus node broadcasts the ViewChange message in the consensus network, the method provided in some embodiments of the present specification further includes the following:

[0039] The second consensus primary node in the consensus network splits, based on the specified erasure coding technology, the target consensus data into the plurality of orderly arranged data fragments that have the same quantity as the consensus nodes in the consensus network, where 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.

[0040] The consensus primary node constructs the Merkle tree based on the plurality of orderly arranged data fragments.

[0041] The second consensus primary node locally saves a data fragment corresponding to the second consensus primary node, a corresponding Merkle tree path, and the root hash of the Merkle tree, and sends, to corresponding consensus nodes in the consensus network, VAL messages including other data fragments, corresponding Merkle tree paths, and the root hash of the Merkle tree, where one data fragment corresponds to one consensus node in the consensus network.

[0042] The Merkle tree path corresponding to the data fragment corresponding to the second consensus primary node is a hash value associated with the data fragment corresponding to the second consensus primary node in the Merkle tree.

[0043] Assume that the quantity of the consensus nodes in the consensus network is 4, before the view change, the consensus network includes the second consensus primary node (consensus node 0) and the consensus backup nodes (consensus node 1 to consensus node 3), where consensus node 3 is abnormal, namely, an abnormal consensus node in the consensus network. Specifically, the second consensus primary node can split the target consensus data into four data fragments (s0 to s3) after processing the target consensus data by using the specified erasure coding algorithm, and the consensus primary node constructs the Merkle tree based on hash values of the split four data fragments (s0 to s3). The hash value of s0 is hash000, the hash value of s1 is hash001, the hash value of s2 is hash002, the hash value of s3 is

hash003, hash (hash00, hash01)=hash00, hash (hash002, hash003)=hash01, and hash (hash01, hash02)=hash0, namely, the root hash of the Merkle tree.

[0044] The consensus primary node locally saves a VAL message including s0, hash value b0 (hash001, hash01) of s0 on the hash path on the Merkle tree, and the root hash hash0 of the Merkle tree, constructs VAL messages based on other data fragments, corresponding Merkle tree paths, and the root hash of the Merkle tree, and sends the VAL messages to consensus nodes corresponding to the data fragment in the VAL messages. Specifically, the consensus primary node can send a first VAL message including (s1 and Hash000, Hash01, Hash0) to consensus node 1, send a second VAL message including (s2 and Hash030, Hash00, Hash0) to consensus node 2, and send a third VAL message including (s3 and Hash020, Hash00, Hash0) to consensus node 3.

[0045] Optionally, after the second consensus primary node locally saves the data fragment corresponding to the second consensus primary node, the corresponding Merkle tree path, and the root hash of the Merkle tree, and sends, to the corresponding consensus nodes in the consensus network, the VAL messages including other data fragments, the corresponding Merkle tree paths, and the root hash of the Merkle tree, the method provided in some embodiments of the present specification further includes the following:

[0046] A third consensus node receiving a VAL message constructs an ECHO message for the received VAL message, and broadcasts the constructed ECHO message to the consensus network, where the constructed ECHO message includes a data fragment, a corresponding Merkle tree path, and the root hash of the Merkle tree in the received VAL message.

[0047] The second consensus primary node constructs an ECHO message based on the locally saved data fragment, corresponding Merkle tree path, and root hash of the Merkle tree, and broadcasts the constructed ECHO message to the consensus network.

[0048] The third consensus node can be any consensus backup node in the consensus network other than the second consensus primary node.

[0049] In some embodiments of the present specification, the message broadcast by the consensus node in the PREPARE stage in the PBFT algorithm is changed to the ECHO message, and the format of the ECHO message is <<ECHO, v, n, r>, bj, sj>. When the consensus node (including the consensus primary node) in the consensus network receives the VAL message; verifies whether the root hash of the Merkle tree

in the VAL data is correct; and if no, discards the message; or if yes, the ECHO message is constructed and broadcast based on the received VAL message and the signature obtained by each consensus node by signing the ECHO message by using the private key.

5 **[0050]** After the consensus node in the consensus network receives $N-2f$ correct ECHO messages, the state of the consensus node can be updated to the VAL complete state. If the consensus node in the consensus network does not receive the VAL message, but receives the $N-2f$ correct ECHO messages sent by the other consensus nodes, the consensus node can obtain the plurality of data fragments and the
10 corresponding Merkle tree by parsing the original target consensus data obtained by parsing the $N-2f$ correct ECHO message sent by the other consensus nodes, construct an ECHO message corresponding to the consensus node based on data fragments corresponding to the present consensus node in the plurality of data fragments, corresponding Merkle tree paths, and the root hash of the Merkle tree, and broadcast
15 the ECHO message and a corresponding signature in the consensus network.

[0051] As shown in FIG.3, FIG. 3 is a schematic diagram illustrating an actual scenario to which a consensus method in a consortium blockchain is applied, according to some embodiments of the present specification. The consensus network shown in the FIG. 3 includes four consensus nodes, that is $N=4$, that is, the second
20 consensus primary node (p0) and the consensus backup nodes (p1 to p3), where p3 is in the abnormal state before view change, and recovers to a normal state after view change.

[0052] In the first stage of the view change vc shown in FIG. 3, when the consensus network does not complete the consensus operation on the target consensus
25 data within the predetermined time period, the first consensus node (any one of consensus nodes p1 to p3) in the consensus network can broadcast the ViewChange message in the consensus network. The format of the ViewChange message is ViewChange (v+1, n, C, P, i).

[0053] Step 220. The first consensus primary node in the consensus network
30 receives the ViewChange message broadcast by the consensus node in the consensus network.

[0054] The first consensus primary node is a consensus primary node corresponding to a view existing when the consensus operation is performed on the target consensus data, i.e., an updated consensus primary node in the consensus

network after the view change. The consensus primary node can be determined by using a formula $p = v \bmod N$, where v is the view number after the view change and N is the quantity of the consensus nodes in the consensus network.

[0055] Step 230. The first consensus primary node constructs a NewView message based on ECHO messages and signatures in $N-f$ verified ViewChange messages when the first consensus primary node determines that the $N-f$ verified ViewChange messages are received, and broadcasts the NewView message to the consensus network to change a view of the consensus network to a target view, where f is a maximum quantity of abnormal consensus nodes allowed in the consensus network, N is a quantity of the consensus nodes in the consensus network, and $N \geq 3f+1$.

[0056] The target view is the next view $v+1$ of the current view v of the consensus network.

[0057] After receiving $N-f$ valid ViewChange messages about changing to the view with the view number $v+1$, the new consensus primary node after the view change, i.e. the first consensus primary node can calculate the NewView message, i.e. content of the NewView message based on the $N-f$ ECHO messages included in the ViewChange message, and add all valid P to O , where the format of O is $\langle v+1, n, r \rangle$, r is the root hash of the Merkle tree constructed by using the plurality of data fragments obtained by splitting the target consensus data, and n is the block number corresponding to the target consensus data. Specifically, when the ViewChange message has a valid P , it indicates that $N-f$ consensus nodes in the consensus network receive the same target consensus data, that is, at least $N-2f$ loyal consensus nodes have a plurality of data fragments corresponding to the target consensus data.

[0058] It can be understood that when the ECHO message broadcast by each consensus node further includes the signature of each consensus node, the legitimacy of the ECHO message can be determined directly based on the signature. Specifically, the step that the first consensus primary node constructs a NewView message based on ECHO messages and signatures in $N-f$ verified ViewChange messages when the first consensus primary node determines that the $N-f$ verified ViewChange messages are received includes the following:

[0059] The first consensus primary node determines 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 the public key.

[0060] When the 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, the first consensus primary node determines that the $N-f$ verified ViewChange messages are received.

5 **[0061]** The first consensus primary node constructs the NewView message based on the ECHO messages and the signatures in the $N-f$ verified ViewChange messages.

[0062] It should be understood that when N data fragments are obtained by splitting the target consensus data by using the specified erasure coding technology, the node need to receive at least $N-2f$ data fragments to recover the original target consensus data. Because P includes $N-f$ Echo messages and signatures, at least $N-2f$ loyal nodes in the system have erasure coding fragments of the target consensus data. Specifically, the step that the first consensus primary node constructs a NewView message based on ECHO messages and signatures in $N-f$ verified ViewChange messages includes the following:

15 **[0063]** The first consensus primary node obtains corresponding $N-f$ data fragments based on the ECHO messages and the signatures in the $N-f$ verified ViewChange messages, and the first consensus primary node constructs the Merkle tree based on the $N-f$ data fragments, and obtains the root hash of the Merkle tree.

[0064] The first consensus primary node constructs the NewView message based on the root hash of the Merkle tree, the $N-f$ verified ViewChange messages, and the block number corresponding to the target consensus data.

[0065] In the previous example in FIG. 3, in the second stage of the view change vc shown in FIG. 3, when determining that the $N-f$ verified ViewChange messages including the ECHO messages and the corresponding signatures are received, first consensus primary node $p1$ can construct the NewView message in the format of NewView ($v+1$, V , O) based on the $N-f$ verified ViewChange messages, and broadcast the NewView message to the consensus network, where V is the $N-f$ ViewChange messages, and O is ($v+1$, n , r) obtained through calculation.

[0066] Step 240. The second consensus node broadcasts 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, where a view number in the ECHO message is a view number of the target view.

[0067] The second consensus node can be any consensus backup node in the consensus network, and the first consensus node and the second consensus node can be the same node or different nodes.

5 **[0068]** The format of the ECHO message for the target consensus data is ECHO (v+1, n, r, bj, sj), where sj is a target data fragment corresponding to the consensus node in the target consensus data, bj is a Merkle tree path of the target data fragment in the Merkle tree, and r is the root hash of the Merkle tree.

10 **[0069]** Optionally, the step that the second consensus node broadcasts 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 includes the following:

15 **[0070]** The second consensus node broadcasts 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 including the root hash of the Merkle tree.

20 **[0071]** Optionally, the step that the second consensus node broadcasts 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 includes the following:

25 **[0072]** 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, the second consensus node constructs 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.

30 **[0073]** The second consensus node that receives the NewView message broadcasts the ECHO message for the target consensus data in the consensus network after the view change.

[0074] As shown in FIG. 3, after the first stage and the second stage of the view change vc are completed, the consensus network enters the normal case phase again.

In this case, the second consensus node that receives the NewView message includes the first consensus primary node. When determining that the present consensus node has the ECHO message corresponding to the target consensus data, i.e. the present consensus node has the target data fragment corresponding to the present consensus
5 node, the second consensus node can construct the ECHO message, namely, ECHO ($v+1$, n , r , b_j , s_j), for the target consensus data based on the target data fragment in the ECHO message corresponding to the target consensus data in the present consensus node, the Merkle tree path of the target data fragment in the Merkle tree, the root hash of the Merkle tree, the view number obtained after the view change, and the block
10 number corresponding to the target consensus data, where s_j is the target data fragment, b_j is the Merkle tree path of the target data fragment in the Merkle tree, and r is the root hash of the Merkle tree. In FIG. 3, consensus node p_3 is the abnormal consensus node in the previous round of consensus operation, but recovers to the normal state after the view change operation, and p_0 is again in a failure state after the
15 view change. Therefore, only consensus nodes p_1 and p_2 have corresponding data fragments in the target consensus data.

[0075] It should be understood that after the second consensus node that receives the NewView message broadcasts the ECHO message for the target consensus data in the consensus network after the view change, the subsequent consensus operation
20 process is unchanged, that is, the method provided in some embodiments of the present specification further includes the following:

[0076] A fourth consensus node that receives the ECHO message for the target consensus data of the $N-f$ consensus nodes commits the target consensus data to a state machine if the fourth consensus node receives ECHO messages of $N-f$
25 consensus nodes for the target consensus data.

[0077] The fourth consensus node can be any consensus node in the consensus network.

[0078] In the consensus method provided in the embodiments of the present specification, when the first consensus node in the consensus network of the
30 consortium blockchain does not complete the consensus operation on the target consensus data within the predetermined time period, the first consensus node can broadcast the ViewChange message in the consensus network based on the ECHO messages broadcast for the target consensus data and the signatures that are sent by other consensus nodes in the consortium blockchain. The first consensus primary

node in the consensus network receives the ViewChange message broadcast by a consensus node in the consensus network. When the first consensus primary node determines that the N-f verified ViewChange messages are received, the first consensus primary node constructs the NewView message based on the ECHO messages and the signatures in the N-f verified ViewChange messages, and broadcasts the constructed NewView message to the consensus network. 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, the second consensus node can broadcast the ECHO message for the target consensus data in the consensus network.

[0079] In other words, after a consensus node in the consensus network triggers a view change operation, any consensus node in the consensus network, i.e. the first consensus node, can broadcast the ViewChange message in the consensus network, and the ViewChange message includes the ECHO messages broadcast by the consensus nodes in the consortium blockchain for the target consensus data and the corresponding signatures that are received by the first consensus node. As such, even if the consensus node triggering the view change is not a consensus primary node after the view change, an ECHO message constructed by the consensus node in the consensus network for the target consensus data and a corresponding signature can still be obtained by other consensus nodes in the consensus network, so that the consensus node in the consensus network continues to perform the consensus operation on the target consensus data in the consensus network after the view change.

[0080] FIG. 4 is a schematic structural diagram illustrating a system 400 in a consortium blockchain, according to some embodiments of the present specification. Referring to FIG. 4, in some software implementations, the system 400 in a consortium blockchain can include a first consensus node 410, a consensus primary node 420, and a second consensus node 430.

[0081] The first consensus node 410 is 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.

[0082] The consensus primary node 420 is configured to receive the ViewChange message broadcast by a consensus node in the consensus network; and construct a NewView message based on ECHO messages and signatures in $N-f$ verified ViewChange messages when the consensus primary node determines that the $N-f$ verified ViewChange messages are received, and broadcast the constructed NewView message to the consensus network to change a view of the consensus network to a target view, where 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 $N \geq 3f+1$.

[0083] The second consensus node 430 is 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, where a view number in the ECHO message is a view number of the target view.

[0084] Based on the system in a consortium blockchain provided in some embodiments of the present specification, the following can be understood:

[0085] After a consensus node in the consensus network triggers a view change operation, any consensus node in the consensus network, i.e. the first consensus node, can broadcast the ViewChange message in the consensus network, and the ViewChange message includes the ECHO messages broadcast by the consensus node in the consortium blockchain for the target consensus data and the corresponding signature that are received by the first consensus node. As such, even if the consensus node triggering the view change is not the consensus primary node after the view change, an ECHO message constructed by the consensus node in the consensus network for the target consensus data and a corresponding signature can still be obtained by other consensus nodes in the consensus network, so that the consensus node in the consensus network continues to perform the consensus operation on the target consensus data in the consensus network after the view change.

[0086] Optionally, in some embodiments, before the first consensus node 410 broadcasts the ViewChange message in the consensus network, the system includes a second consensus primary node 440, configured to split 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, where 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; construct the Merkle tree based on the plurality of orderly arranged data fragments; and locally save a data fragment corresponding to the second consensus primary node, a corresponding Merkle tree path, and a root hash of the Merkle tree, and send, to corresponding consensus nodes
5 in the consensus network, VAL messages including other data fragments, corresponding Merkle tree paths, and the root hash of the Merkle tree, where one data fragment corresponds to one consensus node in the consensus network.

[0087] Optionally, in some embodiments, after the second consensus primary node 440 locally saves the data fragment corresponding to the second consensus primary
10 node, the corresponding Merkle tree path, and the root hash of the Merkle tree, and sends, to the corresponding consensus nodes, the VAL messages including other data fragments, the corresponding Merkle tree paths, and the root hash of the Merkle tree in the consensus network, a third consensus node 450 in the system in a consortium
15 blockchain constructs an ECHO message for the received VAL message, and broadcasts the constructed ECHO message to the consensus network, where the constructed ECHO message includes a data fragment, a corresponding Merkle tree path, and the root hash of the Merkle tree in the received VAL message; and the
20 second consensus primary node 440 constructs an ECHO message based on the locally saved data fragment, corresponding Merkle tree path, and root hash of the Merkle tree, and broadcasts the constructed ECHO message to the consensus network.

[0088] Optionally, in some embodiments, the consensus primary node 420 is configured to determine 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
25 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, determine that the N-f verified ViewChange messages are received; and construct the NewView message based on the ECHO messages and the
signatures in the N-f verified ViewChange messages.

[0089] Optionally, in some embodiments, the consensus primary node 420 is
30 configured to obtain corresponding N-f data fragments based on the ECHO messages and the signatures in the N-f verified ViewChange messages; construct the Merkle tree based on the N-f data fragments, and obtain the root hash of the Merkle tree; and construct 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.

[0090] Optionally, in some embodiments, when receiving the NewView message, the second consensus node 430 is further configured to broadcast the ECHO message for the target consensus data in the consensus network when determining that the present consensus node has an ECHO message including the root hash of the Merkle tree.

[0091] Optionally, in some embodiments, when receiving the NewView message, the second consensus node 430 is further configured to: when determining that the present consensus node has the ECHO message corresponding to the target consensus data, construct 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 broadcast the ECHO message for the target consensus data in the consensus network after the view change.

[0092] Optionally, in some embodiments, the second consensus node 430 broadcast the ECHO message for the target consensus data in the consensus network after the view change, the system further includes: a fourth consensus node 460, configured to commit the target consensus data to a state machine if the fourth consensus node that receives the ECHO message for the target consensus data receives the ECHO messages of the N-f consensus nodes for the target consensus data.

[0093] Optionally, in some embodiments, the first consensus node 410 is any consensus node in the consensus network; and the second consensus node 430 is any consensus node in the consensus network.

[0094] The system 400 in a consortium blockchain can implement the methods provided in method embodiments according to FIG. 2 and FIG. 3, with particular reference to the consensus methods in a consortium blockchain of some embodiments shown in FIG. 2 and FIG. 3, and details are omitted.

[0095] In conclusion, the previous descriptions are merely preferred embodiments of the present specification, and are not intended to limit the scope of protection of the present specification. Any modification, equivalent substitution, improvement, etc. made within the spirit and principles of one or more embodiments of the present

specification shall fall within the scope of the one or more embodiments of the present specification.

[0096] The systems, apparatuses, modules, or units illustrated in the previous embodiments can be implemented by using a computer chip or an entity, or can be implemented by using a product having a certain function. A typical implementation is a computer. Specifically, the computer can be a personal computer, a laptop computer, a cellular phone, a camera phone, a smart phone, a personal digital assistant, a media player, a navigation device, an email receiving and sending device, a game console, a tablet computer, a wearable device, or any combination of these devices.

[0097] A computer readable medium includes persistent, non-persistent, movable, and unmovable media that can save information by using any method or technology. The information can be a computer readable instruction, a data structure, a program module, or other data. Examples of the computer storage medium include but are not limited to a phase change random access memory (PRAM), a static RAM (SRAM), a dynamic RAM (DRAM), a RAM of another type, a read-only memory (ROM), an electrically erasable programmable ROM (EEPROM), a flash memory or another memory technology, a compact disc ROM (CD-ROM), a digital versatile disc (DVD), or another optical storage, a cassette, a cassette magnetic disk storage, or another magnetic storage device or any other non-transmission medium. The computer storage medium can be configured to store information that can be accessed by a computing device. As described in the present application, the computer readable medium does not include computer readable transitory media such as a modulated data signal and a carrier.

[0098] It is worthwhile to note that the terms "comprise", "include", or any other variation thereof are intended to cover a non-exclusive inclusion, so that a process, a method, an article, or a device that includes a list of elements includes those elements and further includes other elements not expressly listed or inherent to such a process, method, product, or device. An element preceded by the phrase "comprise a..." does not, without more constraints, preclude the existence of additional identical elements in the process, method, product, or device that includes the element.

[0099] The embodiments in the present specification are described in a progressive way. For same or similar parts of the embodiments, references can be made to the embodiments. Each embodiment focuses on a difference from other embodiments. Particularly, the system embodiments are similar to method embodiments, and
5 therefore are described briefly. For a related part, references can be made to some descriptions in the method embodiments.

CLAIMS

What is claimed is:

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

5 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
10 nodes in the consensus network;

receiving, by the 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 a consensus primary node corresponding to a view existing when the consensus operation is performed on the target consensus
15 data;

constructing, by the first consensus primary node, a NewView message based on ECHO messages and signatures in $N-f$ verified ViewChange messages when the first consensus primary node determines that the $N-f$ verified ViewChange messages are received, and broadcasting the constructed NewView message to the consensus
20 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
25 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
30 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;

5 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
10 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
15 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
20 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
25 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 based on ECHO messages and
30 signatures in N-f verified ViewChange messages 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 based on ECHO messages and signatures in N-f verified ViewChange messages 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;

a consensus primary node, configured to receive the ViewChange message broadcast by the first consensus node in the consensus network; and construct a NewView message based on ECHO messages and signatures in $N-f$ verified ViewChange messages when the consensus primary node determines that the $N-f$ verified ViewChange messages are received, 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

- 5 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.