

CLAIMS

1. A transaction data processing method, the method being performed by a first consensus node in a blockchain network, and the method comprising:

executing, in response to receiving an initial transaction, the initial transaction to obtain an initial transaction execution record corresponding to the initial transaction,

adding the initial transaction execution record to a first transaction execution data set, the first transaction execution data set being used for recording the initial transaction execution record corresponding to each transaction received by the first consensus node;

adding the initial transaction to a first transaction pool;

acquiring transaction data from the first transaction pool that contains the initial transaction, the transaction data comprising respective initial transaction execution record corresponding to each transaction in a transaction list containing the initial transaction from the first transaction pool, the respective initial transaction corresponding to each transaction in the transaction list being acquired from the first transaction execution data set, wherein the transaction data comprises an initial transaction execution record corresponding to each transaction in the transaction list in the first transaction execution data set, a target transaction execution result corresponding to a verifiable transaction, a target transaction read-write set, and a first block height associated with a first block that is acquired by the first consensus node from the blockchain network in response to executing the verifiable transaction;

generating a proposal block based on the transaction list and the transaction data, the proposal block being subject to block consensus with a second consensus node in the blockchain network, and

performing the block consensus on the proposal block to obtain a block consensus result of the proposal block based on conflict detection, wherein the conflict detection comprises:

determining that a transaction in the transaction list is the verifiable transaction and that a local transaction execution record corresponding to the verifiable transaction is local transaction data associated with the verifiable transaction, wherein the local transaction data comprises a local transaction execution result corresponding to the verifiable transaction, a local transaction read-write set, and a second block height associated with a second block that is acquired from the blockchain network by the second consensus node in response to executing the verifiable transaction;

comparing the target transaction execution result with the local transaction execution result to obtain a first comparison result;

based on the first comparison result indicating that the target transaction execution result is same as the local transaction result, comparing the first block height with the second block height to obtain a second comparison result;

obtaining a local verification result corresponding to the proposal block based on the second comparison result; and

determining a second consensus result corresponding to the proposal block based on the local verification result.

2. The method according to claim 1, wherein the executing comprises:

acquiring, in response to receiving the initial transaction, an initial service contract for executing the initial transaction;

reading an initial read data set corresponding to the initial transaction from the blockchain network based on the initial service contract;

executing the initial transaction based on the initial read data set to obtain an initial transaction execution result corresponding to the initial transaction;

writing the initial transaction execution result into an initial write data set corresponding to the initial transaction,

generating an initial transaction read-write set corresponding to the initial transaction based on the initial read data set and the initial write data set;

determining a first target block that has an initial maximum generation timestamp in response to executing the initial transaction, wherein a block height of the first target block is an initial block height; and

determining the initial transaction execution record based on the initial transaction execution result, the initial transaction read-write set, and the initial block height.

3. The method according to claim 1, wherein the generating the proposal block comprises:

obtaining a Merkle tree root corresponding to a verifiable transaction based on a hash operation on the verifiable transaction and the transaction data, wherein a transaction in the transaction list is the verifiable transaction;

acquiring a block having an initial maximum generation timestamp from the blockchain

network to obtain a second target block; and

generating the proposal block based on verifiable transaction, the transaction data, the Merkle tree root, and a block hash value of the second target block.

4. The method according to claim 1, wherein the performing block consensus further comprises:

determining the block consensus result of the proposal block based on the second consensus result.

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

based on the block consensus result indicating a successful consensus, determining that a consensus on the proposal block is reached;

responsive to the consensus being reached, writing the proposal block into the blockchain as a third target block; and

updating an account state version number corresponding to a transaction object associated with the transaction list.

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

performing validity verification on the initial transaction to obtain a validity verification result;

based on the validity verification result indicates that the initial transaction is valid, determining that the initial transaction passes the validity verification; and

broadcasting the initial transaction that passes the validity verification to the second consensus node, so that the second consensus node executes the initial transaction that passes the validity verification.

7. The method according to claim 6, wherein performing validity verification comprises:

acquiring transaction signature information of the initial transaction and a device public key of a terminal device that transmits the initial transaction, the transaction signature information being obtained after the terminal device signs the initial transaction through a device private key corresponding to the device public key;

obtaining a transaction signature verification result by verifying the transaction signature information based on the device public key;

obtaining a double spending verification result by verifying the initial transaction; and

determining the validity verification result based on the transaction signature verification result and the double spending verification result.

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

based on the transaction signature verification result indicating a signature verification success and the double spending verification result indicating no double spending attack, determining that the initial transaction is valid.

9. A transaction data processing method, the method performed by a second consensus node in a blockchain network, and the method comprising:

receiving a proposal block broadcast by a first consensus node in the blockchain network, the proposal block being based on a transaction list and transaction data associated with the transaction list, wherein the transaction list is acquired by the first consensus node from a first transaction pool of the first consensus node, and the transaction list contains an initial transaction, and wherein the transaction data comprises an initial transaction execution record corresponding to each transaction in the transaction list in a first transaction execution data set, a target transaction execution result corresponding to a verifiable transaction, a target read-write set, and a first block height associated with a first block that is acquired by the first consensus node from the blockchain network in response to executing the verifiable transaction;

obtaining a second consensus result of the proposal block by performing conflict detection on the proposal block based on a conflict detection policy, wherein the conflict detection comprises:

determining that a transaction in the transaction list is the verifiable transaction and that a local transaction execution record corresponding to the verifiable transaction is local transaction data associated with the verifiable transaction, wherein the local transaction data comprises a local transaction execution result corresponding to the verifiable transaction, a local transaction read-write set, and a second block height associated with a second block that is acquired from the blockchain network by the second consensus node in response to executing the verifiable transaction;

comparing the target transaction execution result with the local transaction execution result to obtain a first comparison result;

based on the first comparison result indicating that the target transaction execution result is same as the local transaction result, comparing the first block height with the second block height to obtain a second comparison result;

obtaining a local verification result corresponding to the proposal block based on the second comparison result; and

determining the second consensus result corresponding to the proposal block based on the local verification result; and

transmitting the second consensus result of the proposal block to the first consensus node.

10. The method according to claim 9, wherein the local transaction execution record is acquired from a second transaction execution data set, wherein the second transaction execution data set is used for recording a local transaction record corresponding to each transaction received by the second consensus node, and wherein the local transaction execution record corresponding to the verifiable transaction is obtained by the second consensus node by executing the verifiable transaction.

11. The method according to claim 10, the first block height having a first maximum generation timestamp, and wherein the second block having a second maximum generation timestamp.12. The method according to claim 11, wherein the first maximum generation timestamp is the same as the second maximum generation timestamp; and

the determining the local verification result corresponding to the proposal block based on the second comparison result comprises:

based on the second comparison result indicating that the first block height is the same as the second block height, comparing the target transaction read-write set with the local transaction read-write set to obtain a third comparison result; and

determining the local verification result corresponding to the proposal block based on the third comparison result.

13. The method according to claim 11, wherein the first maximum generation timestamp is different from the second maximum generation timestamp; wherein the target transaction read-write set comprises a first account state version number, the first account state version number being an account version number that is associated with the verifiable transaction and that has a first maximum update timestamp, and the first account state version number being acquired by the first consensus node from the blockchain network in response to executing the verifiable transaction; and wherein the local transaction read-write set comprises a second account state version number, the second account state version number being an account state version number that is associated with the verifiable transaction and that has a second maximum update timestamp, and the second account state version number being acquired by the second consensus node from the blockchain

network in response to executing the verifiable transaction to be verified; and

the determining the local verification result corresponding to the proposal block based on the second comparison result comprises:

based on the second comparison result indicating that the first block height is different from the second block height, comparing the first account state version number with the second account state version number to obtain a fourth comparison result;

based on the fourth comparison result indicating that the first account state version number is different from the second account state version number, acquiring a third account state version number associated with the verifiable transaction and that has a third maximum update timestamp, and comparing the first account state version number with the third account state version number to obtain a fifth comparison result;

based on the fifth comparison result indicating that the third account state version number is lower than the first account state version number, obtaining an updated transaction execution result by re-executing the verifiable transaction;

comparing the target transaction execution result with the updated transaction execution result to obtain a sixth comparison result; and

determining the local verification result corresponding to the proposal block based on the sixth comparison result.

14. The method according to claim 9, wherein the conflict detection comprises:

obtaining an association verification result by verifying the transaction list;

acquiring at least two associated transactions having an association relationship from the transaction list based on the association verification result;

acquiring respective transaction read-write sets corresponding to the at least two associated transactions from the transaction data;

obtaining a read-write set conflict detection result by performing read-write set conflict detection on the respective transaction read-write sets; and

determining the second consensus result corresponding to the proposal block based on the read-write set conflict detection result.

15. A transaction data processing apparatus, comprising:

an execution adding module, configured to, in response to receiving an initial transaction,

execute the initial transaction to obtain an initial transaction execution record corresponding to the initial transaction, add the initial transaction execution record to a first transaction execution data set, the first transaction execution data set being used for recording the initial transaction execution record corresponding to each transaction received by a first consensus node; and add the initial transaction to a first transaction pool;

a data acquisition module, configured to acquire transaction data from the first transaction pool that contains the initial transaction, the transaction data comprising respective initial transaction execution record corresponding to each transaction in a transaction list containing the initial transaction from the first transaction pool, the respective initial transaction corresponding to each transaction in the transaction list being acquired from the first transaction execution data set, wherein the transaction data comprises an initial transaction execution record corresponding to each transaction in the transaction list in the first transaction execution data set, a target transaction execution result corresponding to a verifiable transaction, a target transaction read-write set, and a first block height associated with a first block that is acquired by the first consensus node from the blockchain network in response to executing the verifiable transaction; and

a packing consensus module, configured to generate a proposal block based on the transaction list and the transaction data, the proposal block being subject to block consensus with a second consensus node in the blockchain network, and perform the block consensus on the proposal block to obtain a block consensus result of the proposal block based on conflict detection, wherein the conflict detection comprises:

determining that a transaction in the transaction list is the verifiable transaction and that a local transaction execution record corresponding to the verifiable transaction is local transaction data associated with the verifiable transaction, wherein the local transaction data comprises a local transaction execution result corresponding to the verifiable transaction, a local transaction read-write set, and a second block height associated with a second block that is acquired from the blockchain network by the second consensus node in response to executing the verifiable transaction;

comparing the target transaction execution result with the local transaction execution result to obtain a first comparison result;

based on the first comparison result indicating that the target transaction execution result is same as the local transaction result, comparing the first block height with the second block height to obtain a second comparison result;

obtaining a local verification result corresponding to the proposal block based on the second comparison result; and

determining a second consensus result corresponding to the proposal block based on the local verification result.

16. A transaction data processing apparatus, comprising:

a receiving module, configured to receiving a proposal block broadcast by a first consensus node in the blockchain network; the proposal block being based on a transaction list and transaction data associated with the transaction list; wherein the transaction list is acquired by a first consensus node from a first transaction pool of the first consensus node, and the transaction list contains an initial transaction, and wherein the transaction data comprises an initial transaction execution record corresponding to each transaction in the transaction list in a first transaction execution data set, a target transaction execution result corresponding to a verifiable transaction, a target read-write set, and a first block height associated with a first block that is acquired by the first consensus node from the blockchain network in response to executing the verifiable transaction; and

a detection module, configured to obtain a second consensus result of the proposal block by performing conflict detection on the proposal block based on a conflict detection policy, wherein the conflict detection comprises:

determining that a transaction in the transaction list is the verifiable transaction and that a local transaction execution record corresponding to the verifiable transaction is local transaction data associated with the verifiable transaction, wherein the local transaction data comprises a local transaction execution result corresponding to the verifiable transaction, a local transaction read-write set, and a second block height associated with a second block that is acquired from the blockchain network by the second consensus node in response to executing the verifiable transaction;

comparing the target transaction execution result with the local transaction execution result to obtain a first comparison result;

based on the first comparison result indicating that the target transaction execution result is same as the local transaction result, comparing the first block height with the second block height to obtain a second comparison result;

obtaining a local verification result corresponding to the proposal block based on the second comparison result; and

determining the second consensus result corresponding to the proposal block based on the local verification result; and

transmitting the second consensus result of the proposal block to the first consensus node.

17. A computer device, comprising a memory and one or more processors, the memory storing computer-readable instructions, the computer-readable instructions, when executed by the processor, enabling the one or more processors to perform operations of the method of any one of claims 1 to 14.

18. One or more non-volatile readable storage media, storing computer-readable instructions, the computer-readable instructions, when executed by one or more processors, enabling the one or more processors to implement operations of the method of any one of claims 1 to 14.

19. A computer program product, comprising computer-readable instructions, the computer readable instructions, when executed by a processor, implementing operations of the method of any one of claims 1 to 14.