

CLAIMS

1. A computer-implemented method, comprising:

obtaining, by a client device of a consortium blockchain that comprises a plurality of nodes, respective addresses of the plurality of nodes;

sending, by the client device, a simplified payment verification (SPV) request to each node of the plurality of nodes based on the respective addresses of the plurality of nodes, wherein each SPV request comprises a digest hash of a transaction, and wherein sending the SPV request to each node of the plurality of nodes comprises:

determining, for each node of the plurality of nodes, whether a number of times of sending the SPV request to the node has reached a threshold, and

in response to determining that the number of times has reached the threshold, sending the SPV request to the node after a predetermined delay;

receiving, at the client device, a respective verification result returned by each node of the plurality of nodes that received the SPV request, wherein the respective verification result is generated by each node based on performing SPV verification of the digest hash to verify whether the transaction is recorded in the consortium blockchain; and

determining, by the client device, credibility of the consortium blockchain based on a consistency degree of the respective verification results returned by the plurality of nodes.

2. The computer-implemented method of claim 1, wherein obtaining the respective addresses of the plurality of nodes in the consortium blockchain comprises: randomly obtaining, by the client device, the respective addresses of the plurality of nodes in the consortium blockchain.

3. The computer-implemented method of claim 1, wherein obtaining the respective addresses of the plurality of nodes in the consortium blockchain comprises: obtaining, by the client device, the respective addresses of the plurality of nodes, the respective addresses each including an address of a node associated with the client device in the consortium blockchain.

4. The computer-implemented method of claim 1, further comprising:

sending, by the client device, a transaction position inquiry request to each node of the plurality of nodes based on the respective addresses of the plurality of nodes, wherein the transaction position inquiry request comprises the digest hash of the transaction;

receiving, at the client device, a respective position inquiry result returned by each node of the plurality of nodes that received the transaction position inquiry request, wherein the respective position inquiry result is generated by each node based on inquiring position information of the transaction that corresponds to the digest hash in the consortium blockchain; and

verifying, by the client device, the credibility of the consortium blockchain comprising transaction information based on a degree of consistency of the respective position inquiry results returned by the plurality of nodes.

5. The computer-implemented method of claim 1, further comprising, prior to obtaining the respective addresses of the plurality of nodes:

determining, by each node of the plurality of nodes in the consortium blockchain, a corresponding whitelist; and

broadcasting, by each node of the plurality of nodes in the consortium blockchain, the corresponding whitelist to other nodes in the consortium blockchain.

6. The computer-implemented method of claim 5, further comprising:

determining, by each node of the plurality of nodes in the consortium blockchain, that a client device identifier included in the SPV request is not in the corresponding whitelist, wherein the SPV request comprises the digest hash of the transaction or the client device identifier or both; and

in response, rejecting to perform the SPV verification.

7. The computer-implemented method of claim 1, further comprising:

determining, by each node of the plurality of nodes in the consortium blockchain, a first number of times that the node has processed a SPV request initiated by other nodes;

determining, by each node of the plurality of nodes in the consortium blockchain, a second number of times that the other nodes have processed a SPV request initiated by the node; and

determining whether to process the SPV request in delay based on the first number of times and the second number of times.

8. A computer-implemented system, comprising:

- one or more computers; and

- one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform operations comprising:

 - obtaining, by a client device of a consortium blockchain that comprises a plurality of nodes, respective addresses of the plurality of nodes;

 - sending, by the client device, a simplified payment verification (SPV) request to each node of the plurality of nodes based on the respective addresses of the plurality of nodes, wherein each SPV request comprises a digest hash of a transaction, and wherein sending the SPV request to each node of the plurality of nodes comprises:

 - determining, for each node of the plurality of nodes, whether a number of times of sending the SPV request to the node has reached a threshold, and

 - in response to determining that the number of times has reached the threshold, sending the SPV request to the node after a predetermined delay;

 - receiving, at the client device, a respective verification result returned by each node of the plurality of nodes that received the SPV request, wherein the respective verification result is generated by each node based on performing SPV verification of the digest hash to verify whether the transaction is recorded in the consortium blockchain; and

- determining, by the client device, credibility of the consortium blockchain based on a consistency degree of the respective verification results returned by the plurality of nodes.

9. The computer-implemented system of claim 8, wherein obtaining the respective addresses of the plurality of nodes in the consortium blockchain comprises: randomly obtaining, by the client device, the respective addresses of the plurality of nodes in the consortium blockchain.

10. The computer-implemented system of claim 8, wherein obtaining the respective addresses of the plurality of nodes in the consortium blockchain comprises: obtaining, by the client device, the respective addresses of the plurality of nodes, the respective addresses each including an address of a node associated with the client device in the consortium blockchain.

11. The computer-implemented system of claim 8, wherein the operations further comprise:

sending, by the client device, a transaction position inquiry request to each node of the plurality of nodes based on the respective addresses of the plurality of nodes, wherein the transaction position inquiry request comprises the digest hash of the transaction;

receiving, at the client device, a respective position inquiry result returned by each node of the plurality of nodes that received the transaction position inquiry request, wherein the respective position inquiry result is generated by each node based on inquiring position information of the transaction that corresponds to the digest hash in the consortium blockchain; and

verifying, by the client device, the credibility of the consortium blockchain comprising transaction information based on a degree of consistency of the respective position inquiry results returned by the plurality of nodes.

12. The computer-implemented system of claim 8, wherein the operations further comprise, prior to obtaining the respective addresses of the plurality of nodes:

determining, by each node of the plurality of nodes in the consortium blockchain, a corresponding whitelist; and

broadcasting, by each node of the plurality of nodes in the consortium blockchain, the corresponding whitelist to other nodes in the consortium blockchain.

13. The computer-implemented system of claim 12, wherein the operations further comprise:

determining, by each node of the plurality of nodes in the consortium blockchain, that a client device identifier included in the SPV request is not in the corresponding whitelist, wherein the SPV request comprises the digest hash of the transaction or the client device identifier or both; and

in response, rejecting to perform the SPV verification.

14. The computer-implemented system of claim 8, wherein the operations further comprise:

determining, by each node of the plurality of nodes in the consortium blockchain, a first number of times that the node has processed a SPV request initiated by other nodes;

determining, by each node of the plurality of nodes in the consortium blockchain, a second number of times that the other nodes have processed a SPV request initiated by the node; and

determining whether to process the SPV request in delay based on the first number of times and the second number of times.

15. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

- obtaining, by a client device of a consortium blockchain that comprises a plurality of nodes, respective addresses of the plurality of nodes;

- sending, by the client device, a simplified payment verification (SPV) request to each node of the plurality of nodes based on the respective addresses of the plurality of nodes, wherein each SPV request comprises a digest hash of a transaction, and wherein sending the SPV request to each node of the plurality of nodes comprises:

- determining, for each node of the plurality of nodes, whether a number of times of sending the SPV request to the node has reached a threshold, and

- in response to determining that the number of times has reached the threshold, sending the SPV request to the node after a predetermined delay;

- receiving, at the client device, a respective verification result returned by each node of the plurality of nodes that received the SPV request, wherein the respective verification result is generated by each node based on performing SPV verification of the digest hash to verify whether the transaction is recorded in the consortium blockchain; and

- determining, by the client device, credibility of the consortium blockchain based on a consistency degree of the respective verification results returned by the plurality of nodes.

16. The non-transitory, computer-readable medium of claim 15, wherein obtaining the respective addresses of the plurality of nodes in the consortium blockchain comprises: randomly obtaining, by the client device, the respective addresses of the plurality of nodes in the consortium blockchain.

17. The non-transitory, computer-readable medium of claim 15, wherein obtaining the respective addresses of the plurality of nodes in the consortium blockchain comprises: obtaining, by the client device, the respective addresses of the plurality of nodes, the respective addresses each including an address of a node associated with the client device in the consortium blockchain.

18. The non-transitory, computer-readable medium of claim 15, wherein the operations further comprise:

sending, by the client device, a transaction position inquiry request to each node of the plurality of nodes based on the respective addresses of the plurality of nodes, wherein the transaction position inquiry request comprises the digest hash of the transaction;

receiving, at the client device, a respective position inquiry result returned by each node of the plurality of nodes that received the transaction position inquiry request, wherein the respective position inquiry result is generated by each node based on inquiring position information of the transaction that corresponds to the digest hash in the consortium blockchain; and

verifying, by the client device, the credibility of the consortium blockchain comprising transaction information based on a degree of consistency of the respective position inquiry results returned by the plurality of nodes.