

CLAIMS

~~1. A method of verifying credibility of a consortium blockchain, wherein after a client device generates a transaction and performs on-chain storage for the transaction by a connected node, the method comprises:~~

1. A computer-implemented method, comprising:

obtaining, by a client device, ~~addresses of~~ of a consortium blockchain that comprises a plurality of nodes ~~in the consortium blockchain,~~ 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 ~~a plurality of nodes,~~ wherein the plurality of nodes, wherein each SPV request comprises a digest hash of ~~the~~ transaction;

~~performing, by any one node receiving, and wherein sending the SPV request, an~~ 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 verification-based on 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 present ~~recorded~~ in the consortium blockchain, ~~and returning a verification result to the client device;~~ 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 ~~respectively.~~

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

comprises: randomly obtaining, by the client device, the respective addresses of the plurality of nodes in the consortium blockchain;~~or,~~

~~3. The computer-implemented method of claim 1, wherein obtaining, by the client device, the~~respective addresses of the plurality of nodes ~~comprising an address of the connected node~~ 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.~~

~~3~~

~~4. The computer-implemented method according to~~ 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;

~~inquiring, by any one node~~

receiving ~~the, 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 ~~corresponding that corresponds~~ to the digest hash in the consortium blockchain ~~respectively based on the digest hash; and returning the position inquiry result to the client device; and~~

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

~~4.~~

~~5. The computer-implemented method according to~~ claim 1, ~~before the client device obtains the~~ 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, ~~the method further comprises:~~ a corresponding whitelist; and

~~determining, by any node in the consortium blockchain, its own whitelist; and~~

broadcasting ~~the, by each node of the plurality of nodes in the consortium blockchain, the corresponding~~ whitelist to other nodes in the consortium blockchain, ~~wherein the other nodes determine whether to perform the SPV verification based on the whitelist; and, after receiving the SPV request, by any one node~~

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

determining, ~~whether the client device identifier comprised by each node of the plurality of nodes in the SPV request is 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 SPV request comprises the digest hash of the transaction and~~ the client device identifier or both; and

in response ~~to the client device identifier comprised in the SPV request is not in the whitelist~~, rejecting to perform the SPV verification.

~~5~~

7. The computer-implemented method ~~according to~~ claim 1, ~~wherein after any one node receives the SPV request, the method further comprises~~comprising:

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

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

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

~~6. The method according to claim 1~~

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 ~~any one~~each node of the plurality of nodes, whether a number of times of sending the SPV request to the node ~~reaches~~has reached a threshold, and ~~if~~

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

~~7. A method of verifying credibility of a consortium blockchain, wherein after a receiving, at the client device generates a transaction and performs on-chain storage for the transaction by a connected node, the method comprises:~~

~~obtaining addresses of a~~, a respective verification result returned by each node of the plurality of nodes ~~in that received the consortium blockchain;~~

~~sending a simplified payment verification (SPV) request to, wherein the plurality of nodes~~respective verification result is generated by each node based on the addresses of the plurality of nodes, wherein the performing SPV request comprises a verification of the digest hash ~~of~~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 ~~respectively.~~

8

~~9. The method according to computer-implemented system of claim 7,8,~~ wherein obtaining the respective addresses of the plurality of nodes in the consortium blockchain comprises:

~~randomly obtaining the,~~ by the client device, the respective addresses of the plurality of nodes in the consortium blockchain;~~or.~~

10. The computer-implemented system of claim 8, wherein obtaining the respective addresses of the plurality of nodes comprising an of the connected node 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.

9

~~11. The method according to computer-implemented system of claim 7,8, wherein the operations further comprising~~comprise:

~~sending a~~

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 ~~to~~ comprises the digest hash of the transaction;

receiving, at the client device, a ~~plurality of nodes based on the addresses~~ respective position inquiry result returned by each node of the plurality of nodes, ~~wherein the transaction position inquiry request comprises the digest hash of that received~~ the transaction;
and

~~verifying the credibility of the consortium blockchain comprising~~ 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 ~~respectively~~.

~~10~~

12. The ~~method according to computer-implemented system of claim 78~~, wherein ~~sending the SPV request to~~ 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 ~~any one~~each node of the plurality of nodes, whether a number of times of sending the SPV request to the node ~~reaches~~has reached a threshold, and ~~if~~ in response to determining that the number of times ~~of sending the SPV request to the node reaches~~has reached the threshold, sending the SPV request to the node ~~in~~after a predetermined delay;

~~11. A method of processing~~receiving, at the client device, a request in a consortium blockchain, wherein when a respective verification result returned by each node is one node in the consortium blockchain, ~~of the method comprises:~~

~~determining, by the node, a user identifier~~plurality of a user of the node and determining a whitelist formed of user identifiers, wherein the user identifier is used to identify a user identity and identify a node connected with the user; and

~~sending the whitelist to other nodes in the consortium blockchain, wherein other nodes determine whether to perform a request sent by a user of a non-self node based on the whitelist, wherein the request comprises a transaction position inquiry~~that received the SPV request or an SPV request, a digest hash of a target transaction is comprised in the request.

12. The method according to claim 11, comprising:

~~receiving, by a node, a request from any user, wherein the request further comprises a user identifier; and~~

~~determining whether the user identifier is in the whitelist, and if the user identifier, wherein the respective verification result is not in the whitelist, rejecting the request generated by each node~~

~~13. The method according to claim 11, further comprising:~~

~~receiving a request from any user, wherein the request further comprises a user identifier; when the user corresponding to the user identifier is a user of a non-self node:~~

~~determining a first processing number of times of the node for the requests initiated by users of other nodes, and determining a second processing number of times of other nodes for the requests initiated by a user of the node; and~~

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

~~14. A system for verifying credibility of a consortium blockchain, comprising a client device and a consortium blockchain network, wherein the consortium blockchain network comprises a plurality of nodes, and after a client device generates a transaction and performs on-chain storage for the transaction by a connected node, the system further comprises:~~

~~obtaining, by the client device, addresses of a plurality of nodes in the consortium blockchain;~~

~~sending a simplified payment verification (SPV) request to the plurality of nodes based on the addresses of the plurality of nodes, wherein the SPV request comprises a digest hash of the transaction;~~

~~performing, by any one node in the consortium blockchain network receiving the SPV request, an SPV verification based on performing SPV verification of the digest hash to verify whether the transaction is presentrecorded in the consortium blockchain, and returning a verification result to the client device; 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 respectively.~~

~~15.~~ 16. The ~~system according to non-transitory, computer-readable medium of claim 14~~15, wherein ~~obtaining the client device randomly obtains the~~respective addresses of the plurality of nodes in the consortium blockchain; ~~or comprises: randomly obtaining, by the client device, the client device obtains the~~respective addresses of the plurality of nodes ~~comprising an address of the connected node~~ 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. ~~16.~~ The ~~system according to non-transitory, computer-readable medium of claim 14~~15, wherein the ~~system operations~~ further ~~comprises~~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 ~~a~~the digest hash of the transaction;

~~inquiring, by any node receiving the~~, 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 ~~a~~the transaction ~~corresponding that corresponds~~ to the digest hash in the consortium blockchain ~~respectively based on the digest hash respectively;~~ and ~~returning a position inquiry result to the client device; and~~

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

~~17.~~ The system according to claim 14, before the client device obtains the addresses of the plurality of nodes in the consortium blockchain, the system further comprises:

~~determining, by any node in the consortium blockchain, its own whitelist and broadcasts the whitelist to other nodes in the consortium blockchain, wherein the other nodes determine whether to perform the SPV verification processing based on the whitelist; and~~

~~after receiving the SPV request, any one node, further comprises:~~

determining, whether the client device identifier comprised in the SPV request is in the whitelist, wherein the SPV request comprises the digest hash of the transaction, or, the SPV request comprises the digest hash of the transaction and the client device identifier; and

in response to the client device identifier comprised in the SPV request is not in the whitelist, rejecting the SPV verification request.

~~18.~~ The system according to claim 14, after any one node receives the SPV, the system further comprises:

determining, by the node, a first processing number of times of the node for the SPV initiated by users of other nodes, and a second processing number of times of the other nodes for the SPV initiated by a user of the node; and

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

19. The system according to claim 14, for any one node of the plurality of nodes, the client device determines whether the number of times of sending the SPV request to the node reaches a threshold, and if the number of times of sending the SPV request to the node reaches the threshold, the SPV request will be sent to the node in delay.

20. An apparatus for verifying credibility of a consortium blockchain, after a client device generates a transaction and performs on-chain storage for the transaction by a connected node, the apparatus comprises:

an obtaining module, configured to obtain addresses of a plurality of nodes in the consortium blockchain;

a sending module, configured to send an SPV request to the plurality of nodes based on the addresses of the plurality of nodes, wherein the SPV request comprises a digest hash of the transaction;

a receiving module, configured to receive verification results returned by the plurality of nodes respectively; and

a verifying module, configured to determine credibility of the consortium blockchain based on a consistency degree of the verification results returned by the plurality of nodes respectively.

21. The apparatus according to claim 20, wherein the obtaining module is configured to randomly obtain the addresses of the plurality of nodes in the consortium blockchain; or obtain the addresses of the plurality of nodes comprising an address of the connected node in the consortium blockchain.

22. The apparatus according to claim 20, further comprising:

the sending module being further configured to send a transaction position inquiry request to the plurality of nodes based on the addresses of the plurality of nodes, wherein the transaction position inquiry request comprises a digest hash of the transaction;

the receiving module being configured to receive position inquiry results returned by the plurality of nodes respectively; and

the verifying module being configured to verify the credibility of the consortium blockchain comprising the transaction information based on a degree of consistency of position inquiry results returned by the plurality of nodes respectively.

23. The apparatus according to claim 20, wherein the sending module is configured to: for any one node of the plurality of nodes, determine whether a number of times of sending the SPV request to the node reaches a threshold; and if the number of times of sending the SPV request to the node reaches the threshold, send the SPV request to the node in delay.

24. An apparatus for processing a request in a consortium blockchain, wherein the apparatus is on a node of the consortium blockchain and comprises:

a determining module, configured to determine, by the node, a user identifier of a user of the node, and determine a whitelist formed of user identifiers, wherein the user identifier is used to identify a user identity and identify a node connected with the user; and

a sending module, configured to send the whitelist to other nodes in the consortium blockchain, wherein the other nodes determine whether to perform a request from a user of a non-self node based on the whitelist, wherein the request comprises a transaction position inquiry request or an SPV, a digest hash of a target transaction is comprised in the request.

~~25. The apparatus according to claim 24, comprising:~~

~~a receiving module, configured to receive a request from any user, wherein the request further comprises a user identifier; and~~

~~a deciding module, configured to determine whether the user identifier is in the whitelist and if the user identifier is not in the whitelist, reject the request.~~

~~26. The apparatus according to claim 24, wherein~~

~~the receiving module receives a request from any user, wherein the request further comprises a user identifier; when the user corresponding to the user identifier is a user of a non-self node;~~

~~the determining module is further configured to determine a first processing number of times of the node for the request initiated by users of other nodes, and a second processing number of times of the other nodes for the request initiated by a user of the node; and~~

~~the deciding module is further configured to determine whether to process the request in delay based on the first processing number of times and the second processing number of times.~~

~~27. A computer device, comprising a memory, a processor and computer programs stored on the memory and operable on the processor, wherein the programs are executed by the processor to implement the method according to any one of claims 7-10.~~

~~28. A computer device, comprising a memory, a processor and computer programs stored on the memory and operable on the processor, wherein the programs are executed by the processor to implement the method according to any one of claims 11-13.~~