

CLAIMS

What is claimed is:

1. ~~__A blockchain-based transaction processing method, applied to a client device,~~
wherein a Nonce list corresponding to a user account is maintained in a blockchain, the
Nonce list comprises a plurality of Nonce records, the Nonce record comprises a version
identifier of the Nonce list and a Nonce value, and the method comprises:

obtaining ~~(202), by a client device,~~ an available Nonce record for a target
transaction initiated by a user through the user account from the Nonce list;

adding ~~(204), by the client device,~~ the obtained available Nonce record to the target
transaction; and

publishing ~~(206), by the client device,~~ the target transaction in the blockchain,~~so
that when;~~

~~receiving (208), by a node device in the blockchain, the target transaction;~~

determining~~that, by the node device, whether~~ a version identifier in the available
Nonce record ~~matches a version identifier of the Nonce list that corresponds to the user
account and is maintained in the blockchain;~~

~~if the version identifier in the available Nonce record~~ does not match the version
identifier of the Nonce list ~~that corresponds to the user account and is~~ maintained in the
blockchain, ~~returning (210), by the node device in the blockchain returns,~~ prompt
information indicating that the target transaction is an invalid transaction to the client
device; ~~or and~~

~~when determining that aif the~~ version identifier in the available Nonce record
matches the version identifier of the Nonce list ~~that corresponds to the user account and
is~~ maintained in the blockchain, ~~the node device in the blockchain~~ further
~~matches~~matching the available Nonce record with ~~thea~~ Nonce record in the Nonce list
to perform replay attack detection for the target transaction, and ~~processes~~processing
~~(212), by the node device,~~ the target transaction when the replay attack detection for the
target transaction succeeds~~;~~

~~wherein if the available Nonce record matches the Nonce record in the Nonce list,
monotonically increasing, by the node device, a Nonce value in the target Nonce record
based on a predetermined amplitude; and~~

returning, by the node device, a notification message indicating that the target transaction is processed to the client device.

2. The method according to claim 1, wherein before the obtaining, by the client device, an available Nonce record for a target transaction initiated by a user through the user account from the Nonce list, the method further comprises:

in response to an initialization instruction for the client device, obtaining the Nonce list maintained in the blockchain, and locally maintaining the obtained Nonce list on the client device.

3. The method according to claim 2, wherein the obtaining, by the client device, an available Nonce record for a target transaction initiated by a user through the user account from the Nonce list comprises:

obtaining the available Nonce record for the target transaction initiated by the user through the user account from the Nonce list locally maintained on the client device.

4. The method according to claim 3, wherein the Nonce record in the Nonce list locally maintained on the client device is marked as available by default; and
the method further comprises:

marking, by the client device, the available Nonce record as unavailable in the Nonce list after obtaining the available Nonce record for the target transaction from the Nonce list locally maintained on the client device.

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

determining, by the client device, whether a notification message indicating that the target transaction is processed is received from the node device; and

if yes, monotonically increasing, by the client device, a Nonce value in the available Nonce record based on predetermined amplitude, and re-marking the available Nonce record as available in the Nonce list after monotonically increasing the Nonce value.

6. The method according to claim 1, wherein the client device is a multi-threaded client device, and a quantity of Nonce records in the Nonce list indicates a transaction concurrency capability of the user account.

7. The method according to claim 1, wherein the Nonce record further comprises an index identifier of the Nonce record.

~~8. A blockchain-based transaction processing method, applied to a node device in a blockchain, wherein a Nonce list set is maintained in the blockchain, the Nonce list set comprises Nonce lists corresponding to several user accounts, the Nonce list comprises a plurality of Nonce records, the Nonce record comprises a version identifier of the Nonce list and a Nonce value, and the method comprises:~~

~~receiving a target transaction that is initiated by a user through a user account and sent by a client device, wherein an available Nonce record obtained from a Nonce list that corresponds to the user account and is maintained in the blockchain is added to the target transaction;~~

~~determining whether a version identifier in the available Nonce record matches a version identifier of the Nonce list that corresponds to the user account and is maintained in the blockchain; and~~

~~if the version identifier in the available Nonce record does not match the version identifier of the Nonce list that corresponds to the user account and is maintained in the blockchain, returning prompt information indicating that the target transaction is an invalid transaction to the client device; or~~

~~if the version identifier in the available Nonce record matches the version identifier of the Nonce list that corresponds to the user account and is maintained in the blockchain, further matching the available Nonce record with a Nonce record in the Nonce list to perform replay attack detection for the target transaction, and processing the target transaction when the replay attack detection for the target transaction succeeds.~~

~~9. The method according to claim 8~~

8. The method according to claim 1, wherein the matching the available Nonce record with a Nonce record in the Nonce list to perform replay attack detection for the target transaction comprises:

matching, by the node device, the available Nonce record with the Nonce record in the Nonce list that corresponds to the user account and is maintained in the blockchain; and

if the available Nonce record matches any target Nonce record in the Nonce list, determining, by the node device, that the replay attack detection for the target transaction succeeds.

~~10. The method according to claim—~~

~~9, further comprising:~~

~~if the available Nonce record matches the any target Nonce record in the Nonce list, monotonically increasing a Nonce value in the target Nonce record based on predetermined amplitude; and~~

~~returning a notification message indicating that the target transaction is processed to the client device.~~

~~11. The method according to claim 9, wherein the Nonce record further comprises an index identifier of the Nonce record.~~

~~12. A blockchain-based transaction processing apparatus, applied to a client device, wherein a Nonce list corresponding to a user account is maintained in a blockchain, the Nonce list comprises a plurality of Nonce records, the Nonce record comprises a version identifier of the Nonce list and a Nonce value, and the apparatus comprises:~~

~~an acquisition module, configured to obtain an available Nonce record for a target transaction initiated by a user through the user account from the Nonce list;~~

~~an addition module, configured to add the obtained available Nonce record to the target transaction; and~~

~~a publication module, configured to publish the target transaction in the blockchain, so that when determining that a version identifier in the available Nonce record does not match the version identifier of the Nonce list maintained in the blockchain, a node device in the blockchain returns prompt information indicating that the target transaction is an invalid transaction to the client device; or when determining that a version identifier in the available Nonce record matches the version identifier of the Nonce list maintained in the blockchain, the node device in the blockchain further matches the available Nonce record with the Nonce record in the Nonce list to perform replay attack detection for the target transaction, and processes the target transaction when the replay attack detection for the target transaction succeeds.~~

~~13. The apparatus according to claim 12, wherein the acquisition module is further configured to:~~

~~before obtaining the available Nonce record for the target transaction initiated by the user through the user account from the Nonce list, in response to an initialization~~

instruction for the client device, obtain the Nonce list maintained in the blockchain, and locally maintain the obtained Nonce list on the client device.

~~14. The apparatus according to claim 13, wherein the acquisition module is configured to:~~

~~obtain the available Nonce record for the target transaction initiated by the user through the user account from the Nonce list locally maintained on the client device.~~

~~15. The apparatus according to claim 14, wherein the Nonce record in the Nonce list locally maintained on the client device is marked as available by default; and~~

~~the acquisition module is further configured to:~~

~~mark the available Nonce record as unavailable in the Nonce list after obtaining the available Nonce record for the target transaction from the Nonce list locally maintained on the client device.~~

~~16. The apparatus according to claim 15, wherein the acquisition module is further configured to:~~

~~determine whether a notification message indicating that the target transaction is processed is received from the node device; and if yes, monotonically increase a Nonce value in the available Nonce record based on predetermined amplitude, and re-mark the available Nonce record as available in the Nonce list after monotonically increasing the Nonce value.~~

~~17. The apparatus according to claim 12, wherein the client device is a multi-threaded client device, and a quantity of Nonce records in the Nonce list indicates a transaction concurrency capability of the user account.~~

~~18. The apparatus according to claim 17, wherein the Nonce record further comprises an index identifier of the Nonce record.~~

~~19. A blockchain-based transaction processing apparatus, applied to a node device in a blockchain, wherein a Nonce list set is maintained in the blockchain, the Nonce list set comprises Nonce lists corresponding to several user accounts, the Nonce list comprises a plurality of Nonce records, the Nonce record comprises a version identifier of the Nonce list and a Nonce value, and the apparatus comprises:~~

~~a receiving module, configured to receive a target transaction that is initiated by a user through a user account and sent by a client device, wherein an available Nonce record obtained from a Nonce list that corresponds to the user account and is maintained in the blockchain is added to the target transaction;~~

~~a determining module, configured to determine whether a version identifier in the available Nonce record matches a version identifier of the Nonce list that corresponds to the user account and is maintained in the blockchain; and~~

~~a return module, configured to: if the version identifier in the available Nonce record does not match the version identifier of the Nonce list that corresponds to the user account and is maintained in the blockchain, return prompt information indicating that the target transaction is an invalid transaction to the client device; or~~

~~a detection module, configured to: if the version identifier in the available Nonce record matches the version identifier of the Nonce list that corresponds to the user account and is maintained in the blockchain, further match the available Nonce record with a Nonce record in the Nonce list to perform replay attack detection for the target transaction, and process the target transaction when the replay attack detection for the target transaction succeeds.~~

20. The apparatus according to claim 19, wherein the detection module is further configured to:

~~match the available Nonce record with the Nonce record in the Nonce list that corresponds to the user account and is maintained in the blockchain; and~~

~~if the available Nonce record matches any target Nonce record in the Nonce list, determine that the replay attack detection for the target transaction succeeds.~~

21. The apparatus according to claim 20, wherein the detection module is further configured to:

~~if the available Nonce record matches the any target Nonce record in the Nonce list, monotonically increase a Nonce value in the target Nonce record based on predetermined amplitude; and~~

~~return a notification message indicating that the target transaction is processed to the client device.~~

22. The apparatus according to claim 21, wherein the Nonce record further comprises an index identifier of the Nonce record.

23. ~~_____~~ An electronic ~~devices~~system, comprising:

a processor; and

a memory, configured to store a machine-executable instruction, wherein

by reading and executing the machine-executable instruction that is stored in the memory and corresponds to blockchain-based transaction processing control logic, the processor is promoted to perform ~~the following operations:~~

~~obtaining an available Nonce record for a target transaction initiated by a user through a user account from a Nonce list that corresponds to the user account and is maintained in a blockchain, wherein the Nonce list comprises a plurality of Nonce records, and the Nonce record comprises a version identifier of the Nonce list and a Nonce value;~~

~~adding the obtained available Nonce record to the target transaction; and~~

~~publishing the target transaction in the blockchain, so that when determining that a version identifier in the available Nonce record does not match the version identifier of the Nonce list maintained in the blockchain, a node device in the blockchain returns prompt information indicating that the target transaction is an invalid transaction to a client device; or when determining that a version identifier in the available Nonce record matches the version identifier of the Nonce list maintained in the blockchain, the node device in the blockchain further matches the available Nonce record with the Nonce record in the Nonce list to perform replay attack detection for the target transaction, and processes the target transaction when the replay attack detection for the target transaction succeeds.~~

~~24. An electronic device, comprising:~~

~~a processor; and~~

~~a memory, configured to store a machine-executable instruction, wherein~~

~~by reading and executing the machine-executable instruction that is stored in the memory and corresponds to blockchain-based transaction processing control logic, the processor is promoted to perform the following operations:~~

~~receiving a target transaction that is initiated by a user through a user account and sent by a client device, wherein an available Nonce record obtained from a Nonce list that corresponds to the user account and is maintained in a blockchain is added to the target transaction, the Nonce list comprises a plurality of Nonce records, and the Nonce record comprises a version identifier of the Nonce list and a Nonce value;~~

~~determining whether a version identifier in the available Nonce record matches the version identifier of the Nonce list that corresponds to the user account and is maintained in the blockchain; and~~

~~if the version identifier in the available Nonce record does not match the version identifier of the Nonce list that corresponds to the user account and is maintained in the blockchain, returning prompt information indicating that the target transaction is an invalid transaction to the client device; or~~

~~if the version identifier in the available Nonce record matches the version identifier of the Nonce list that corresponds to the user account and is maintained in the blockchain, further matching the available Nonce record with the Nonce record in the Nonce list to perform replay attack detection for the target transaction, and processing the target transaction when the replay attack detection for the target transaction succeeds;~~a method according to any one of the preceding claims.