

CLAIMS:

1. A computer-implemented method for detecting a replay attack without using an account nonce, wherein the method is performed by a blockchain node of a blockchain, the method comprising:

pooling a plurality of identifications of a plurality of candidate transactions by synchronizing an identification database of the blockchain node with one or more identification databases of one or more different blockchain nodes of the blockchain or receiving one or more of the plurality of candidate transactions from the one or more different blockchain nodes, wherein before the pooling, the plurality of candidate transactions were received by the blockchain node and the one or more different blockchain nodes during a time period starting from a time point when a newest block of the blockchain was added to the blockchain;

storing the pooled identifications of the plurality of candidate transactions in the identification database of the blockchain node;

obtaining a candidate transaction for adding to a blockchain, the obtained candidate transaction comprising a timestamp of the candidate transaction, transaction information of the candidate transaction, and an identification of the candidate transaction, wherein the identification of the candidate transaction comprises a hash value of at least the timestamp of the candidate transaction and the transaction information of the candidate transaction;

verifying the identification of the candidate transaction by verifying the hash value based at least on the timestamp of the candidate transaction and the transaction information of the candidate transaction;

determining if the timestamp of the candidate transaction is within a validation range corresponding to the time period and if the identification of the candidate transaction exists in the identification database of the blockchain node; and

in response to determining that the timestamp of the candidate transaction is within the validation range and the identification of the candidate transaction does not exist in the identification database of the blockchain node, determining that the candidate transaction is not associated with a replay attack.

2. The method of claim 1, wherein: the blockchain node is a primary node of a PBFT (Practical Byzantine Fault Tolerance) system.

3. The method of claim 1, further comprising:
removing, from the identification database of the blockchain node, one or more identifications of one or more candidate transactions that are received by any of the blockchain node and the one or more different blockchain nodes outside the validation range.

4. The method of claim 1, wherein:

obtaining the candidate transaction for adding to the blockchain comprises receiving the candidate transaction from a user terminal, the received candidate transaction comprising the timestamp of the candidate transaction.

5. The method of claim 1, wherein obtaining the candidate transaction for adding to the blockchain comprises:

receiving a transaction without the timestamp of the candidate transaction from a user terminal; and

adding the timestamp of the candidate transaction to the received transaction to obtain the candidate transaction

.

6. The method of claim 1, further comprising:

in response to determining that the timestamp of the candidate transaction is within the validation range and the identification of the candidate transaction does not exist in the identification database of the candidate transaction, adding the identification to the identification database.

7. The method of claim 1, further comprising:

in response to determining that the timestamp of the candidate transaction is within the validation range and the identification of the candidate transaction does not exist in the identification database of the blockchain node, adding the candidate transaction to a cache for storing candidate transactions.

8. The method of claim 1, further comprising:

in response to determining that the timestamp of the candidate transaction is not within the validation range, returning an error message to a computing device that submitted the candidate transaction.

9. The method of claim 1, further comprising:

in response to determining that the identification of the candidate transaction exists in the identification database of the blockchain node, determining that the candidate transaction is associated with the replay attack.

10. The method of claim 1, further comprising:

performing consensus verification on the candidate transaction determined not to be associated with the replay attack.

11. The method of claim 10, further comprising:

synchronizing the identification database of the blockchain node with one or more identification databases of the one or more different blockchain nodes of the blockchain;

verifying if the timestamp of the candidate transaction is within the validation range and if the identification of the candidate transaction exists in the synchronized identification database;

in response to determining that the timestamp of the candidate transaction is within the validation range and the identification of the candidate transaction does not exist in the synchronized identification database, determining that the candidate transaction is not associated with the replay attack; and

in response to determining that the identification of the candidate transaction exists in the synchronized identification database, determining that the candidate transaction is associated with the replay attack.

12. The method of claim 1, before obtaining the at least one candidate transaction, further comprising:

synchronizing the identification database of the blockchain node with one or more identification databases of the one or more other blockchain nodes of the blockchain.

13. The method of claim 1, wherein:

a duration of the validation range corresponds to a duration between adding two consecutive blocks to the blockchain

14. The method of claim 1, wherein:

the validation range is included in a genesis block of the blockchain.

15. The method of claim 1, wherein:

the validation range is based on an internal clock of a blockchain node of the blockchain that performs the verifying if the timestamp of the candidate transaction is within the validation range.

16. A system for detecting a replay attack without using an account nonce, comprising one or more processors and one or more non-transitory computer-readable memories coupled to the one or more processors and configured with instructions executable by the one or more processors to cause the system to perform operations comprising:

pooling a plurality of identifications of a plurality of candidate transactions by synchronizing an identification database of a blockchain node of a blockchain with one or more identification databases of one or more different blockchain nodes of the blockchain or receiving one or more of the plurality of candidate transactions from the one or more different blockchain nodes, wherein before the pooling, the plurality of candidate transactions were received by the blockchain node and the one or more different blockchain nodes during a time period starting from a time point when a newest block of the blockchain was added to the blockchain;

storing the pooled identifications of the plurality of candidate transactions in the identification database of the blockchain node; obtaining a candidate transaction for adding to a blockchain, the obtained candidate transaction comprising a timestamp of the candidate transaction, transaction information of the candidate transaction, and an identification of the candidate transaction, wherein the identification of the candidate transaction comprises a hash value of at least the timestamp of the candidate transaction and the transaction information of the candidate transaction;

verifying the identification of the candidate transaction by verifying the hash value based at least on the timestamp of the candidate transaction and the transaction information of the candidate transaction; determining if the timestamp of the candidate transaction is within a validation range corresponding to the time period and if the identification of the candidate transaction exists in the identification database of the blockchain node; and

in response to determining that the timestamp of the candidate transaction is within the validation range and the identification of the candidate transaction does not exist in the identification database of the blockchain node, determining that the candidate transaction is not associated with a replay attack.

17. The system of claim 16, wherein:
the blockchain node is a primary node of a PBFT (Practical Byzantine Fault Tolerance) system.

18. A non-transitory computer-readable storage medium configured with instructions executable by one or more processors to cause the one or more processors to perform operations comprising:

pooling a plurality of identifications of a plurality of candidate transactions by synchronizing an identification database of a blockchain node of a blockchain with one or more identification databases of one or more different blockchain nodes of the blockchain or receiving one or more of the plurality of candidate transactions from the one or more different blockchain nodes, wherein before the pooling, the plurality of candidate transactions were received by the blockchain node and the one or more different blockchain nodes during a time period starting from a time point when a newest block of the blockchain was added to the blockchain;

obtaining a candidate transaction for adding to a blockchain, the obtained candidate transaction comprising a timestamp of the candidate transaction, transaction information of the candidate transaction, and an identification of the candidate transaction, wherein the identification of the candidate transaction comprises a hash value of at least the timestamp of the candidate transaction and the transaction information of the candidate transaction;

verifying the identification of the candidate transaction by verifying the hash value based at least on the timestamp of the candidate transaction and the transaction information of the candidate transaction;

determining if the timestamp of the candidate transaction is within a validation range corresponding to the time period and if the identification of the candidate transaction exists in the identification database of the blockchain node; and

in response to determining that the timestamp of the candidate transaction is within the validation range and the identification of the candidate transaction does not exist in the identification database of the blockchain node, determining that the candidate transaction is not associated with a replay attack.

19. The storage medium of claim 18, wherein:
the blockchain node is a primary node of a PBFT (Practical Byzantine Fault Tolerance) system.

20. The storage medium of claim 18, wherein the operations further comprise:
removing, from the identification database of the blockchain node, one or more identifications of one or more candidate transactions that are received by any of the blockchain node and the one or more different blockchain nodes outside the validation range.