

What Is Claimed Is

1 1. A computer-executed method for processing a transaction based on
2 blockchain, the method comprising:
3 sending, by a first node associated with the blockchain, a transaction
4 confirmation request for a target transaction to a second node associated with the
5 blockchain, wherein the transaction confirmation request comprises transaction
6 data associated with the target transaction, and wherein the transaction data
7 comprises identifying information of the first node's user associated with the
8 target transaction;
9 receiving a transaction confirmation response from the second node,
10 wherein the transaction confirmation response comprises a first data block and
11 first signature, wherein the first data block comprises an identifier of the second
12 node, a first piece of encoded transaction data generated by
13 encoding the transaction data based on a predetermined encoding scheme,
14 and a first confirmation result, wherein the first signature corresponds to a
15 signature computed on the first data block using a private key of the second node,
16 and wherein the first confirmation result indicates approval of the target
17 transaction by the second node based on the identifying information;
18 generating, by the first node, a second data block comprising at least an
19 identifier of the first node, a second piece of encoded transaction data generated
20 by encoding the transaction data based on the predetermined encoding scheme,
21 and a second confirmation result indicating approval of the target transaction by
22 the first node;
23 computing, by the first node, a second signature, which is computed on the
24 second data block using a private key of the first node; and
25 in response to both the first and second confirmation results indicating that
26 the target transaction is confirmed:

1 storing the first and second data blocks in the blockchain, thereby
2 preventing the transaction data from being leaked to other members in the
3 blockchain; and
4 storing the first and second signatures in the blockchain along with
5 the first and second data blocks, respectively.

6 2. The method according to claim 1, further comprising:
7 in response to both the first and second confirmation results indicating that
8 the target transaction is confirmed, processing the target transaction for the
9 blockchain.

10 3. The method according to claim 2, wherein processing the target
11 transaction further comprises:
12 recording processing result information of the target transaction; and
13 sending the processing result information to a respective node associated
14 with the target transaction through the blockchain, thereby allowing the node to
15 process the target transaction.

16
17 4. The method according to claim 1, wherein
18 storing the first and second data blocks in the blockchain further
19 comprises:
20 storing the first data block, the first signature, the second data block, and
21 the second signature in a same block.

22 5. The method according to claim 1, further comprising verifying the
23 first signature and the second signature.

24

25

1 6. The method according to claim 1, wherein storing the first and
2 second data blocks in the blockchain further comprises:
3 checking whether the identifier of the second node and the identifier of the
4 first node are associated with the target transaction;
5 checking whether the first piece of encoded transaction data matches the
6 second piece of encoded transaction data; and
7 in response to the identifier of the second node and the identifier of the
8 first node being associated with the target transaction, and the first piece of
9 encoded transaction data matching the second piece of encoded transaction data,
10 storing both the first data block and the second data block in the blockchain.

11 7. A computer-executed method for processing a transaction based on
12 blockchain, the method comprising:
13 receiving, by a first node associated with the blockchain, a transaction
14 confirmation request for a target transaction from a second node associated with
15 the blockchain, wherein the transaction confirmation request comprises
16 transaction data associated with the target transaction, and wherein the transaction
17 data comprises identifying information of the second node's user associated with
18 the target transaction;
19 generating a first confirmation result based on the transaction data,
20 wherein the first confirmation result indicates approval of the target transaction by
21 the first node based on the identifying information;
22 generating a first piece of encoded transaction data by encoding the
23 transaction data using a predetermined encoding scheme;
24 computing a first signature, which is computed on the first data block
25 using a private key of the first node;
26 sending, by the first node, a transaction confirmation response to the
27 second node, wherein the transaction confirmation response comprises a first data

1 block and the first signature, wherein the first data block comprises an identifier
2 of the first node, the first encoded transaction data, and the first confirmation
3 result, thereby facilitating the second node in storing the first data block in the
4 blockchain in response to determining that the target transaction is confirmed
5 based on the first confirmation result and preventing the transaction data from
6 being leaked to other members in the blockchain.

7 8. The method according to claim 7, further comprising:
8 receiving result information of the target transaction from the blockchain;
9 and
10 processing the target transaction according to the result information.

11 9. The method according to claim 7, further comprising:
12 storing the first signature in the blockchain along with the first data block.

13 10. A computer system, comprising
14 a processor;
15 a storage device coupled to the processor and storing instructions, which
16 when executed by the processor cause the processor to perform a method for
17 processing a transaction based on blockchain, the method comprising:
18 sending, by a first node associated with the blockchain, a
19 transaction confirmation request for a target transaction to a second node
20 associated with the blockchain, wherein the transaction confirmation
21 request comprises transaction data associated with the target transaction,
22 and wherein the transaction data comprises identifying information of the
23 first node's user associated with the target transaction;
24 receiving a transaction confirmation response from the second
25 node, wherein the transaction confirmation response comprises a first data
26 block and a first signature, wherein the first data block comprises an
27 identifier of the second node, a first piece of encoded transaction data

1 generated by encoding the transaction data based on a predetermined
2 encoding scheme, and a first confirmation result, wherein the first
3 signature corresponds to a signature computed on the first data block using
4 a private key of the second node, and wherein the first confirmation result
5 indicates approval of the target transaction by the second node based on
6 the identifying information;

7 generating, by the first node, a second data block comprising at
8 least an identifier of the first node, a second piece of encoded transaction
9 data generated by encoding the transaction data based on the
10 predetermined encoding scheme, and a second confirmation result
11 indicating approval of the target transaction by the first node;

12 computing, by the first node, a second signature, which is
13 computed on the second data block using a private key of the first node;
14 and

15 in response to both the first and second confirmation results
16 indicating that the target transaction is confirmed:

17 storing the first and second data blocks in the blockchain,
18 thereby preventing the transaction data from being leaked to other
19 members in the blockchain; and

20 storing the first and second signatures in the blockchain
21 along with the first and second data blocks, respectively.

22 11. The computer system according to claim 10, wherein the method
23 further comprises:

24 in response to determining that both the first and second confirmation
25 results indicating that the target transaction is confirmed, processing the target
26 transaction for the blockchain.

27 12. The computer system according to claim 11, wherein processing
28 the target transaction further comprises:

1 recording result information of the target transaction; and
2 sending the result information to a respective node associated with the
3 target transaction through the blockchain, thereby allowing the node to process
4 the target transaction.

5

6 13. The computer system according to claim 10, wherein storing the
7 first and second data blocks in the blockchain further comprises:

8 storing the first data block, the first signature, the second data block, and
9 the second signature in a same block.

10

11 14. The computer system according to claim 10, wherein the method
12 further comprising verifying the first signature and the second signature.

13

14 15. The computer system according to claim 10, wherein storing the
15 first and second data blocks in the blockchain further comprises:

16 checking whether the identifier of the second node and the
17 identifier of the first node are associated with the target transaction;

18 checking whether the first piece of encoded transaction data matches the
19 second piece of encoded transaction data; and

20 in response to the identifier of the second node the identifier of the first
21 node being associated with the target transaction and the first piece of encoded
22 transaction data matching the second piece of encoded transaction data, storing
23 both the first data block and the second data block in the blockchain.

24

25 16. A non-transitory computer-readable storage medium storing
26 instructions that when executed by a computer cause the computer to perform a
27 method for processing a transaction based on blockchain, the method comprising:

28 sending, by a first node associated with the blockchain, a transaction
29 confirmation request for a target transaction to a second node associated with the

1 blockchain, wherein the transaction confirmation request comprises transaction
2 data associated with the target transaction, and wherein the transaction data
3 comprises identifying information of the first node's user associated with the
4 target transaction;

5 receiving a transaction confirmation response from the second node,
6 wherein the transaction confirmation response comprises a first data block and a
7 first signature, wherein the first data block comprises an identifier of the second
8 node, a first piece of encoded transaction data generated by encoding the
9 transaction data based on a predetermined encoding scheme, and a first
10 confirmation result, wherein the first signature corresponds to a signature
11 computed on the first data block using a private key of the second node, and
12 wherein the first confirmation result indicates approval of the target transaction by
13 the second node based on the identifying information;

14 generating, by the first node, a second data block comprising at least an
15 identifier of the first node, a second piece of encoded transaction data generated
16 by encoding the transaction data based on the predetermined encoding scheme,
17 and a second confirmation result indicating approval of the target transaction by
18 the first node;

19 computing, by the first node, a second signature, which is computed on the
20 second data block using a private key of the first node; and

21 in response to both the first confirmation result and the second
22 confirmation result indicating that the target transaction is confirmed:

23 storing the first and second data blocks in the blockchain, thereby
24 preventing the transaction data from being leaked to other members in the
25 blockchain; and

26 storing the first and second signatures in the blockchain along with
27 the first and second data blocks, respectively.

28

1 17. The non-transitory computer-readable storage medium according
2 to claim 16, wherein the method further comprises:
3 in response to both the first and second confirmation results indicating that
4 the target transaction is confirmed, processing the target transaction for the
5 blockchain.

6
7 18. The non-transitory computer-readable storage medium according
8 to claim 17, wherein processing the target transaction further comprises:
9 recording result information of the target transaction; and
10 sending the result information to a respective node associated with the
11 target transaction through the blockchain, thereby allowing the node to process
12 the target transaction.

13
14 19. The non-transitory computer-readable storage medium according
15 to claim 16, wherein storing the first and second data blocks in the blockchain
16 further comprises:
17 storing the first data block, the first signature, the second data block, and
18 the second signature in a same block.

19 20. The non-transitory computer-readable storage medium according
20 to claim 16, wherein the method further comprises verifying the first signature
21 and the second signature.

22 21. The non-transitory computer-readable storage medium according
23 to claim 16, wherein storing the first and second data blocks in the blockchain
24 further comprises:
25 checking whether the identifier of the second node and the identifier of the
26 first node are associated with the target transaction;
27 checking whether the first piece of encoded transaction data matches the
28 second piece of encoded transaction data; and

1 in response to the identifier of the second node and the identifier of the
2 first node being associated with the target transaction, and the first piece of
3 encoded transaction data matching the second encoded piece of transaction data,
4 storing both the first data block and the second data block in the blockchain.
5