

What Is Claimed Is

1 1. A computer-executed transaction processing method for processing
2 a transaction based on blockchain, the method being performed by a transaction
3 initiator and comprising:

4 sending, by a first node associated with the blockchain, a transaction
5 confirmation request for a target transaction to a second node associated with the
6 blockchain, wherein each transaction-related party, the transaction confirmation
7 request comprises transaction data associated with the target transaction, and
8 wherein the transaction data comprises identifying information of the first node's
9 user associated with the target transaction;

10 receiving a transaction confirmation response from each of the second
11 node transaction-related parties, wherein the transaction confirmation response
12 comprises a first data block and first signature data, wherein the first data
13 block comprises first encoded data generated by encoding the transaction data
14 using a preset encoding method by the transaction-related party, a first
15 confirmation result, and an identifier of the second node transaction-related party,
16 and the first piece of encoded transaction signed data is obtained generated by
17 performing signature computation on the first data block by using a private key of
18 the transaction-related party;

19 encoding the transaction data based on a predetermined using the preset
20 encoding scheme, and a first method to generate second encoded data; and
21 generating a second confirmation result, wherein the first signature corresponds to
22 a signature computed on the first data block using a private key of the second
23 node, and wherein the first confirmation result indicates approval of the target
24 transaction by the second node based on the identifying information;

25 generating, by the first node, a second data block comprising at least an
26 identifier of the first node, a second piece of encoded transaction data generated

1 by encoding the transaction data based on the predetermined encoding scheme,
2 and a second confirmation result indicating approval of the target transaction by
3 the first node;
4 computingsigning, by the first node, a second signature, which is
5 computed onusing a private key of the transaction initiator, a the second data
6 block using a private key of the first nodecomprising the second encoded data, the
7 second confirmation result, and an identifier of the transaction initiator, so as to
8 obtain second signed data; and
9 _____ in response to both the first and second confirmation results indicating that
10 the target transaction is confirmed:
11 _____ storing the first and second data blocks_ and the first signed data of
12 each of the transaction related parties and the second data block and the
13 second signed data of the transaction initiator through a in the blockchain,
14 thereby preventing the transaction data from being leaked to other
15 members in the blockchain; and
16 _____ storing the first and second signatures in the blockchain along with
17 the first and second data blocks, respectivelynetwork when determining
18 that each of the first confirmation results and the second confirmation
19 result are Confirmed.

20 2. The method according to claim 1, further comprising:
21 in response to bothprocessing the target transaction through the blockchain
22 network when determining that each of the first and second confirmation results
23 indicating that the target transaction is and the second confirmation result are
24 cConfirmed, processing the target transaction for the blockchain.

25 3. The method according to claim 2, wherein processing the target
26 transaction further through the blockchain network comprises:
27 recording processing result information of the target transaction through
28 the blockchain network; and

1 sending the processing result information of the target transaction to a
2 respective node associated with the target ~~each of the transaction-related parties~~
3 through the blockchain network, thereby allowing the node to so ~~that each of the~~
4 ~~transaction-related parties~~ processes the target transaction.

5 4.—— A transaction processing method, the method being performed by a
6 ~~transaction-related party and comprising:~~

7 —— ~~receiving a transaction confirmation request for a target transaction from a~~
8 ~~transaction initiator, the transaction confirmation request comprising transaction~~
9 ~~data;~~

10 —— ~~generating a first confirmation result according to the transaction data;~~

11 —— ~~encoding the transaction data using a preset encoding method to generate~~
12 ~~first encoded data;~~

13 —— ~~signing, by using a private key of the transaction-related party, a first data~~
14 ~~block comprising the first confirmation result and the first encoded data, so as to~~
15 ~~obtain first signed data; and~~

16 —— ~~sending a transaction confirmation response to the transaction initiator, the~~
17 ~~transaction confirmation response comprising the first data block and the first~~
18 ~~signed data, so that the transaction initiator stores the first data block and the first~~
19 ~~signed data of each of the transaction-related parties and data of the transaction~~
20 ~~initiator through a blockchain network when determining that a confirmation~~
21 ~~result of each of the transaction-related parties is Confirmed.~~

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

23 —— ~~receiving processing result information of the target transaction from the~~
24 ~~blockchain network; and~~

25 —— ~~processing the target transaction according to the processing result~~
26 ~~information.~~

1 46. TheA transaction processing method according to claim 1, wherein
2 the method being performed by a blockchain network and comprising:
3 —receiving, from a transaction initiator of a target transaction, a first data
4 block and first signed data of each transaction-related party and a second data
5 block and second signed data of the transaction initiator, wherein the first data
6 block comprises first encoded data generated by encoding transaction data using a
7 preset encoding method by the transaction-related party, a first confirmation
8 result, and an identifier of the transaction-related party; the first signed data is
9 obtained by performing signature computation on the first data block by using a
10 private key of the transaction-related party; the second data block comprises
11 second encoded data generated by encoding the transaction data using the preset
12 encoding method by the transaction initiator, a second confirmation result, and an
13 identifier of the transaction initiator; and the second signed data is obtained by
14 performing signature computation on the second data block by using a private key
15 of the transaction initiator; and
16 storing the first and second data blocks in the blockchain further
17 comprises:
18 —storing and the first signed data block, the first signature, of each of the
19 transaction-related parties and the second data block, and the second signature
20 in a same blockdata of the transaction initiator.

21 57. The method according to claim 16, wherein, after storing the first
22 data block and the first signed data of each of the transaction-related parties and
23 the second data block and the second signed data of the transaction initiator, the
24 method further comprising verifying the first signature and the second
25 signature.es:
26 processing the target transaction.

1 8. ~~—— The method according to claim 7, wherein processing the target~~
2 ~~transaction comprises:~~
3 ~~—— recording processing result information of the target transaction; and~~
4 ~~—— sending the processing result information of the target transaction to each~~
5 ~~of the transaction-related parties, so that each of the transaction-related parties~~
6 ~~processes the target transaction.~~

7 69. The method according to claim 17, wherein, ~~before storing the first~~
8 ~~and second data blocks in the blockchain and the first signed data of each of the~~
9 ~~transaction-related parties and the second data block and the second signed data of~~
10 ~~the transaction initiator, the method further comprises:~~

11 ~~performing the following checks:~~

12 ~~checking whether the identifier of the second node transaction-related party~~
13 ~~and/or the identifier of the first node are associated with transaction initiator~~
14 ~~matches a member identifier on a transaction link of the target transaction;~~

15 ~~checking whether each of the first piece of encoded transaction data~~
16 ~~matches the same as the second piece of encoded transaction data; and~~

17 ~~in response to the identifier of the second node and the identifier of~~
18 ~~performing signature verification on the first node being associated with data~~
19 ~~block and the first signed data of each of the target transaction, -related parties by~~
20 ~~using a public key of each of and the first piece of encoded transaction-related~~
21 ~~parties to verify whether the first data block matching the first signed data; and~~
22 ~~—— performing signature verification on the second data block and the second~~
23 ~~piece of encoded transaction signed data, storing both the first of the transaction~~
24 ~~initiator by using a public key of the transaction initiator to verify whether the~~
25 ~~data block and the second data block in the blockchain matches the second signed~~
26 ~~data; and~~

27 ~~determining that checking results of the checks are all Yes.~~

1 10.——The method according to claim 6, wherein storing the first data
2 block and the first signed data of each of the transaction-related parties and the
3 second data block and the second signed data of the transaction initiator
4 comprises:
5 ——storing the first data block and the first signed data of each of the
6 transaction-related parties and the second data block and the second signed data of
7 the transaction initiator in a block.

8 11.——A transaction processing apparatus, the apparatus being deployed
9 at a transaction initiator and comprising:
10 ——a sending unit, configured to send a transaction confirmation request for a
11 target transaction to each transaction-related party, the transaction confirmation
12 request comprising transaction data;
13 ——a receiving unit, configured to receive a transaction confirmation response
14 from each of the transaction-related parties, the transaction confirmation response
15 comprising a first data block and first signed data, wherein the first data block
16 comprises first encoded data generated by encoding the transaction data using a
17 preset encoding method by the transaction-related party, a first confirmation
18 result, and an identifier of the transaction-related party; and the first signed data is
19 obtained by performing signature computation on the first data block by using a
20 private key of the transaction-related party;
21 ——an encoding unit, configured to encode the transaction data using the
22 preset encoding method to generate second encoded data; and generate a second
23 confirmation result;
24 ——a signing unit, configured to sign, by using a private key of the transaction
25 initiator, a second data block comprising the second encoded data, the second
26 confirmation result, and an identifier of the transaction initiator, so as to obtain
27 second signed data; and
28 a storage unit, configured to store the first data block and the first signed

1 data of each of the transaction-related parties that are received by the receiving
2 unit and the second data block and the second signed data of the transaction
3 initiator through a blockchain network, when it is determined that each of the first
4 confirmation results received by the receiving unit and the second confirmation
5 result generated by the encoding unit are Confirmed.

6 12.—The apparatus according to claim 11, further comprising:
7 —a processing unit, configured to process the target transaction through the
8 blockchain network when it is determined that each of the first confirmation
9 results received by the receiving unit and the second confirmation result are
10 Confirmed.

11 13.—The apparatus according to claim 12, wherein the processing unit
12 is specifically configured to:
13 —record processing result information of the target transaction through the
14 blockchain network; and
15 —send the processing result information of the target transaction to each of
16 the transaction-related parties through the blockchain network, so that each of the
17 transaction-related parties processes the target transaction.

18 14. A computer-executed method for transaction processing apparatus,
19 the apparatus being deployed at a transaction based on blockchain-related party
20 and the method comprising:

21 a receiving unit, by a first node associated with the blockchain, configured
22 to receive a transaction confirmation request for a target transaction from a second
23 node transaction initiator associated with the blockchain, wherein the transaction
24 confirmation request comprises transaction data associated with the target
25 transaction, and wherein the transaction data comprises identifying information of
26 the second node's user associated with the target transaction;

1 a confirmation unit, configured to generating a first confirmation result
2 based on ~~according to~~ the transaction data, wherein the first confirmation result
3 indicates approval of the target transaction by the first node based on the
4 identifying information received by the receiving unit;
5 generating a first piece of an encoding unit, configured to encoded the
6 transaction data received by the receiving unit using a preset encoding method to
7 generate first encoded the transaction data using a predetermined encoding
8 scheme;
9 computing a first signature, which is computed on the first data block a
10 signing unit, configured to sign, by using a private key of the first
11 node; transaction-related party, a first data block comprising the first confirmation
12 result and the first encoded data, so as to obtain first signed data; and
13 a sending unit, by the first node, configured to send a transaction
14 confirmation response to the second node ~~transaction initiator, wherein the~~
15 transaction confirmation response comprises ~~ing at~~ the first data block and the first
16 signed data, wherein ~~so that the transaction initiator stores the first data block~~
17 comprises an identifier of and the first node, the first encoded transaction data, and
18 the first signed data of each of the transaction-related parties and data of the
19 transaction initiator through a blockchain network when determining that a
20 confirmation result, thereby facilitating the second node in storing the first data
21 block in the blockchain in response to determining that the target transaction is
22 confirmed based on the first confirmation result and preventing the transaction
23 data from being leaked to other members in the blockchain of each of the
24 transaction-related parties is Confirmed.

25 845. The method apparatus according to claim 744, further
26 comprising wherein:

27 the receiving unit is further configured to receive processing result
28 information of the target transaction from the blockchain network; and

29 the apparatus further comprises:

1 a processing unit, configured to process the target transaction according to
2 the processing result information received by the receiving unit.

3 16. — A transaction processing apparatus, the apparatus being deployed
4 in a blockchain network and comprising:
5 —— a receiving unit, configured to receive, from a transaction initiator of a
6 target transaction, a first data block and first signed data of each transaction-
7 related party and a second data block and second signed data of the transaction
8 initiator, wherein the first data block comprises first encoded data generated by
9 encoding transaction data using a preset encoding method by the transaction-
10 related party, a first confirmation result, and an identifier of the transaction-
11 related party; the first signed data is obtained by performing signature
12 computation on the first data block by using a private key of the transaction-
13 related party; the second data block comprises second encoded data generated by
14 encoding the transaction data using the preset encoding method by the transaction
15 initiator, a second confirmation result, and an identifier of the transaction initiator;
16 and the second signed data is obtained by performing signature computation on
17 the second data block by using a private key of the transaction initiator; and
18 —— a storage unit, configured to store the first data block and the first signed
19 data of each of the transaction-related parties and the second data block and the
20 second signed data of the transaction initiator that are received by the receiving
21 unit.

22 917. The methodapparatus according to claim 716, further comprising:
23 a processing unit, configured to process the target transaction after the
24 storage unit stores the first data block and the first signatureed in the
25 blockchain along with the first data of each of the transaction-related parties and
26 the second data block and the second signed data of the transaction initiator.

27 10. A computer system, comprising

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

1 in response to both the first and second confirmation results
2 indicating that the target transaction is confirmed:
3 storing the first and second data blocks in the blockchain,
4 thereby preventing the transaction data from being leaked to other
5 members in the blockchain; and
6 storing the first and second signatures in the blockchain
7 along with the first and second data blocks, respectively.

8 ~~1148. The computer system~~~~apparatus~~ according to claim 1017, wherein
9 the method further comprises ~~processing unit is specifically configured to:~~
10 in response to determining that both the first and second
11 confirmation~~record processing results~~ indicating that~~information of the target~~
12 transaction is confirmed; ~~and~~
13 ~~send the processing result information of the target transaction for the~~
14 blockchain~~to each of the transaction-related parties, so that each of the~~
15 ~~transaction-related parties processes the target transaction.~~

16 12. The computer system according to claim 11, wherein processing
17 the target transaction further comprises:
18 recording result information of the target transaction; and
19 sending the result information to a respective node associated with the
20 target transaction through the blockchain, thereby allowing the node to process
21 the target transaction.

22
23 13. The computer system according to claim 10, wherein storing the
24 first and second data blocks in the blockchain further comprises:
25 storing the first data block, the first signature, the second data block, and
26 the second signature in a same block.

27

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

3 _____
4 1519. The computer system apparatus according to claim 1017, wherein
5 storing the first and second data blocks in the blockchain further comprising:
6 ~~a checking unit, configured to perform the following checks before the~~
7 ~~storage unit stores the first data block and the first signed data of each of the~~
8 ~~transaction-related parties and the second data block and the second signed data of~~
9 ~~the transaction initiator:~~

10 ~~checking whether the identifier of the second node transaction-related party~~
11 ~~and/or the identifier of the first node transaction initiator matches a member~~
12 ~~identifier on a transaction link of are associated with the target transaction;~~

13 ~~checking whether each of the first piece of encoded transaction data~~
14 ~~matches is the same as the second piece of encoded transaction data; and~~

15 ~~in response to the identifier of the second node the identifier of the first~~
16 ~~node being associated with the target transaction and the first piece of encoded~~
17 ~~transaction data matching the second piece of encoded transaction data, storing~~
18 ~~both the first data block and the second data block in the blockchain~~

19 ~~performing signature verification on the first data block and the first~~
20 ~~signed data of each of the transaction-related parties by using a public key of each~~
21 ~~of the transaction-related parties to verify whether the first data block matches the~~
22 ~~first signed data; and~~

23 ~~performing signature verification on the second data block and the second~~
24 ~~signed data of the transaction initiator by using a public key of the transaction~~
25 ~~initiator to verify whether the second data block matches the second signed data;~~
26 ~~and~~

27 ~~a determining unit, configured to determine that checking results of the~~
28 ~~checks obtained by the check unit are all Yes.~~

1 20. — The apparatus according to claim 16, wherein the storage unit is
2 specifically configured to store, in a block, the first data block and the first signed
3 data of each of the transaction-related parties and the second data block and the
4 second signed data of the transaction initiator that are received by the receiving
5 unit.

6 1621. A non-transitory computer-readable storage medium storing
7 instructions that, having a computer program stored thereon, wherein when
8 executed by a computer, the computer program causes the computer to perform
9 the method for processing a transaction based on blockchain, the method
10 comprising: according to any one of claims 1 to 10
11 sending, by a first node associated with the blockchain, a transaction
12 confirmation request for a target transaction to a second node associated with the
13 blockchain, wherein the transaction confirmation request comprises transaction
14 data associated with the target transaction, and wherein the transaction data
15 comprises identifying information of the first node's user associated with the
16 target transaction;
17 receiving a transaction confirmation response from the second node,
18 wherein the transaction confirmation response comprises a first data block and a
19 first signature, wherein the first data block comprises an identifier of the second
20 node, a first piece of encoded transaction data generated by encoding the
21 transaction data based on a predetermined encoding scheme, and a first
22 confirmation result, wherein the first signature corresponds to a signature
23 computed on the first data block using a private key of the second node, and
24 wherein the first confirmation result indicates approval of the target transaction by
25 the second node based on the identifying information;
26 generating, by the first node, a second data block comprising at least an
27 identifier of the first node, a second piece of encoded transaction data generated
28 by encoding the transaction data based on the predetermined encoding scheme,

1 and a second confirmation result indicating approval of the target transaction by
2 the first node;
3 computing, by the first node, a second signature, which is computed on the
4 second data block using a private key of the first node; and
5 in response to both the first confirmation result and the second
6 confirmation result indicating that the target transaction is confirmed:
7 storing the first and second data blocks in the blockchain, thereby
8 preventing the transaction data from being leaked to other members in the
9 blockchain; and
10 storing the first and second signatures in the blockchain along with
11 the first and second data blocks, respectively.

12
13 17. The non-transitory computer-readable storage medium according
14 to claim 16, wherein the method further comprises:
15 in response to both the first and second confirmation results indicating that
16 the target transaction is confirmed, processing the target transaction for the
17 blockchain.

18
19 18. The non-transitory computer-readable storage medium according
20 to claim 17, wherein processing the target transaction further comprises:
21 recording result information of the target transaction; and
22 sending the result information to a respective node associated with the
23 target transaction through the blockchain, thereby allowing the node to process
24 the target transaction.

25
26 19. The non-transitory computer-readable storage medium according
27 to claim 16, wherein storing the first and second data blocks in the blockchain
28 further comprises:

1 storing the first data block, the first signature, the second data block, and
2 the second signature in a same block.

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

6 21. The non-transitory computer-readable storage medium according
7 to claim 16, wherein storing the first and second data blocks in the blockchain
8 further comprises:

9 checking whether the identifier of the second node and the identifier of the
10 first node are associated with the target transaction;

11 checking whether the first piece of encoded transaction data matches the
12 second piece of encoded transaction data; and

13 in response to the identifier of the second node and the identifier of the
14 first node being associated with the target transaction, and the first piece of
15 encoded transaction data matching the second encoded piece of transaction data,
16 storing both the first data block and the second data block in the blockchain.

17 ~~22. A computing device, comprising a memory and a processor,~~
18 ~~wherein the memory stores executable code, and when the processor executes the~~
19 ~~executable code, the method according to any one of claims 1 to 10 is~~
20 ~~implemented.~~