

CLAIMS

What is claimed is:

1. A method for executing a smart contract of a blockchain, wherein the blockchain is interconnected to a trusted third party, a contract engine for executing a smart contract
5 is deployed in the trusted third party, and the method comprises:

receiving, by a node device in the blockchain, a target transaction initiated by a client device to invoke a target smart contract;

obtaining contract source code of the target smart contract from a distributed database of the blockchain in response to the target transaction, wherein the target
10 transaction comprises an input parameter; and

~~sending the contract source code to the trusted third party so that the contract engine of the trusted third party executes the contract source code and returns an execution result to the node device;~~

sending the contract source code to the trusted third party so that the contract
15 engine of the trusted third party executes the contract source code, comprising:

sending the contract source code and the input parameter to the trusted third party, so that the trusted third party obtains input data corresponding to the input parameter from the node device, loads the input data into the contract source code, and executes the contract source code;

20 wherein the blockchain is interconnected to another trusted third party that serves as a verification party;

the method further comprises:

sending the execution result to the another trusted third party, so that a contract engine of the another trusted third party verifies the execution result;

25 in response to determining that the verification on the execution result succeeds, publishing the execution result to all node devices in the blockchain for consensus processing, and storing the execution result in the blockchain after the consensus succeeds;

wherein the execution result is a result set generated by the trusted third party
30 based on an execution result of the contract source code, and the result set comprises a read-write set generated in a process of executing the contract source code and an execution result obtained after the contract source code is executed;

a verification process for the execution result comprises:

reading, by the contract engine of the another trusted third party, input data from the read-write set, loading the read input data into the contract source code, and simulating execution of the contract source code;

- 5 determining whether an execution result generated by simulating execution of the contract source code is consistent with the execution result in the result set; and
in response to determining that the execution result generated by simulating execution of the contract source code is consistent with the execution result in the result set, determining that the verification on the execution result succeeds.

- 10 2. A method for executing a smart contract of a blockchain, wherein the blockchain is interconnected to a trusted third party, a contract engine for executing a smart contract is deployed in the trusted third party, and the method comprises:

receiving, by a node device in the blockchain, a target transaction initiated by a client device to invoke a target smart contract;

- 15 obtaining contract source code of the target smart contract from a distributed database of the blockchain in response to the target transaction, wherein the target transaction comprises an input parameter;

sending the contract source code to the trusted third party so that the contract engine of the trusted third party executes the contract source code, comprising:

- 20 sending the contract source code and the input parameter to the trusted third party, so that the trusted third party obtains input data corresponding to the input parameter from the node device, loads the input data into the contract source code, and executes the contract source code;

- wherein the blockchain is interconnected to another trusted third party that serves
25 as a verification party;

the method further comprises:

sending the execution result to the another trusted third party, so that a contract engine of the another trusted third party verifies the execution result;

- in response to determining that the verification on the execution result succeeds,
30 publishing the execution result to all node devices in the blockchain for consensus processing, and storing the execution result in the blockchain after the consensus succeeds;

wherein the execution result is a result set generated by the trusted third party based on an execution result of the contract source code, and the result set comprises a

read-write set generated in a process of executing the contract source code and an execution result obtained after the contract source code is executed;

a verification process for the execution result comprises:

5 reading, by the contract engine of the another trusted third party, input data from the read-write set, loading the read input data into the contract source code, and simulating execution of the contract source code;

determining whether a read-write set generated by simulating execution of the contract source code is consistent with the read-write set in the result set; and

10 in response to determining that the read-write set generated by simulating execution of the contract source code is consistent with the read-write set in the result set, determining that the verification on the execution result succeeds.

~~2.3.~~ The method according to claim 1 or 2, wherein the target transaction comprises a target smart contract name and a name of a target function invoked in the target smart contract; and

the obtaining contract source code of the target smart contract from a distributed database of the blockchain specifically comprises:

obtaining contract source code corresponding to the target smart contract name from the distributed database of the blockchain based on the target smart contract name comprised in the target transaction; and

obtaining contract source code corresponding to the name of the target function from the obtained contract source code based on the name of the target function invoked in the target smart contract.

~~3. The method according to claim 1, wherein the transaction comprises an input parameter; and~~

~~the sending the contract source code to the trusted third party so that the contract engine of the trusted third party executes the contract source code comprises:~~

~~sending the contract source code and the input parameter to the trusted third party, so that the trusted third party obtains input data corresponding to the input parameter from the node device, loads the input data into the contract source code, and executes the contract source code.~~

~~4. The method according to claim 3, wherein the blockchain is interconnected to another trusted third party that serves as a verification party; and~~

~~the method further comprises:~~

~~sending the execution result to the another trusted third party, so that a contract engine of the another trusted third party verifies the execution result; and~~

~~in response to determining that the verification on the execution result succeeds, publishing the execution result to all node devices in the blockchain for consensus processing, and storing the execution result in the blockchain after the consensus succeeds.~~

~~5. The method according to claim 4, wherein~~

~~a verification process for the execution result comprises:~~

~~reading, by the contract engine of the another trusted third party, input data from the read-write set, loading the read input data into the contract source code, and simulating execution of the contract source code;~~

~~determining whether an execution result generated by simulating execution of the contract source code is consistent with the execution result in the result set; and~~

~~in response to determining that the execution result generated by simulating execution of the contract source code is consistent with the execution result in the result set, determining that the verification on the execution result succeeds.~~

~~6. The method according to claim 4, wherein~~

~~a verification process for the execution result comprises:~~

~~reading, by the contract engine of the another trusted third party, input data from the read-write set, loading the read input data into the contract source code, and simulating execution of the contract source code;~~

~~determining whether a read-write set generated by simulating execution of the contract source code is consistent with the read-write set in the result set; and~~

~~in response to determining that the read-write set generated by simulating execution of the contract source code is consistent with the read-write set in the result set, determining that the verification on the execution result succeeds.~~

~~7.4. The method according to claim 1 or 2, wherein the blockchain is a consortium blockchain.~~

~~8.5. A method for executing a smart contract of a blockchain, wherein the blockchain is interconnected to a trusted third party, a contract engine for executing a smart contract is deployed in the trusted third party, and the method comprises:~~

~~receiving, by the contract engine of the trusted third party, contract source code sent by a node device in the blockchain, wherein the node device is a node that responds to a target transaction request initiated by a client device to invoke a target smart~~

contract in the blockchain, and the contract source code is contract source code of the target smart contract;

~~executing the contract source code and returning an execution result to the node device; and~~

5 wherein the method further comprises:

 when receiving a verification request sent by the node device for a result set of a contract engine of another trusted third party, verifying the result set, wherein the result set comprises a read-write set generated in a process of executing the contract source code and an execution result obtained after the contract source code is executed;

10

in response to determining that the verification on the result set succeeds, publishing the execution result in the result set to all node devices in the blockchain for consensus processing, and storing the execution result in the result set in the blockchain after the consensus succeeds;

15 wherein a verification process for the second execution result comprises:

reading input data from the read-write set, loading the read input data into the contract source code, and simulating execution of the contract source code;

determining whether an execution result generated by simulating execution of the contract source code is consistent with the execution result in the result set;

20 and

in response to determining that the execution result generated by simulating execution of the contract source code is consistent with the execution result in the result set, determining that the verification on the execution result succeeds.

25 6. A method for executing a smart contract of a blockchain, wherein the blockchain is interconnected to a trusted third party, a contract engine for executing a smart contract is deployed in the trusted third party, and the method comprises:

receiving, by the contract engine of the trusted third party, contract source code sent by a node device in the blockchain, wherein the node device is a node that responds to a target transaction request initiated by a client device to invoke a target smart contract in the blockchain, and the contract source code is contract source code of the target smart contract;

30

wherein the method further comprises:

when receiving a verification request sent by the node device for a result set of a contract engine of another trusted third party, verifying the result set, wherein the result

set comprises a read-write set generated in a process of executing the contract source code and an execution result obtained after the contract source code is executed;

in response to determining that the verification on the result set succeeds, publishing the execution result in the result set to all node devices in the blockchain for consensus processing, and storing the execution result in the result set in the blockchain after the consensus succeeds;

wherein a verification process for the second execution result comprises:

reading input data from the read-write set, loading the read input data into the contract source code, and simulating execution of the contract source code;

determining whether a read-write set generated by simulating execution of the contract source code is consistent with the read-write set in the result set; and

in response to determining that the read-write set generated by simulating execution of the contract source code is consistent with the read-write set in the result set, determining that the verification on the execution result succeeds.

9.7. The method according to claim 8 or 6, wherein the transaction comprises an input parameter;

the receiving contract source code sent by a node device in the blockchain specifically comprises:

receiving the contract source code and the input parameter that are sent by the node device in the blockchain; and

the executing the contract source code specifically comprises:

obtaining input data corresponding to the input parameter from the node device, loading the input data into the contract source code, and executing the contract source code.

~~10. The method according to claim 8, wherein the method further comprises:~~

~~in response to determining that the verification on the result set succeeds, publishing the execution result in the result set to all node devices in the blockchain for consensus processing, and storing the execution result in the result set in the blockchain after the consensus succeeds.~~

~~11. The method according to claim 10, wherein a verification process for the second execution result comprises:~~

~~reading input data from the read-write set, loading the read input data into the contract source code, and simulating execution of the contract source code;~~

determining whether an execution result generated by simulating execution of the contract source code is consistent with the execution result in the result set; and

in response to determining that the execution result generated by simulating execution of the contract source code is consistent with the execution result in the result set, determining that the verification on the execution result succeeds.

12. The method according to claim 10, wherein a verification process for the second execution result comprises:

reading input data from the read-write set, loading the read input data into the contract source code, and simulating execution of the contract source code;

determining whether a read-write set generated by simulating execution of the contract source code is consistent with the read-write set in the result set; and

in response to determining that the read-write set generated by simulating execution of the contract source code is consistent with the read-write set in the result set, determining that the verification on the execution result succeeds.

13.8. The method according to claim 85 or 6, wherein the blockchain is a consortium blockchain.

14. An apparatus for executing a smart contract of a blockchain, wherein the blockchain is interconnected to a trusted third party, a contract engine for executing a smart contract is deployed in the trusted third party, and the apparatus comprises:

a receiving unit, configured to receive a target transaction initiated by a client device to invoke a target smart contract;

a response unit, configured to obtain contract source code of the target smart contract from a distributed database of the blockchain in response to the target transaction; and

an execution unit, configured to send the contract source code to the trusted third party so that the contract engine of the trusted third party executes the contract source code and returns an execution result to the node device, wherein the execution result is a result set generated by the trusted third party based on an execution result of the contract source code, and the result set comprises a read-write set generated in a process of executing the contract source code and an execution result obtained after the contract source code is executed.

15. An apparatus for executing a smart contract of a blockchain, wherein the blockchain is interconnected to a trusted third party, a contract engine for executing a smart contract is deployed in the trusted third party, and the apparatus comprises:

~~a receiving unit, configured to receive contract source code sent by a node device in the blockchain, wherein the node device is a node that responds to a target transaction request initiated by a client device to invoke a target smart contract in the blockchain, and the contract source code is contract source code of the target smart contract;~~

5 ~~an execution unit, configured to execute the contract source code and return an execution result to the node device; and~~

~~a verification unit, configured to, when receiving a verification request sent by the node device for a result set of a contract engine of another trusted third party, verify the result set, wherein the result set comprises a read-write set generated in a process of~~
10 ~~executing the contract source code and an execution result obtained after the contract source code is executed.~~

~~16.9.~~ An electronic device, comprising:

a processor; and

a memory configured to store processor-executable instructions, wherein

15 the processor is configured to perform the method according to any one of claims

1 to ~~13~~8.