

CLAIMS

What is claimed is:

1. A blockchain smart contract-based signature verification method, wherein the method comprises:

5 adding, to an instruction set of a blockchain virtual machine that is associated with a blockchain network and that does not support an RSA signature verification operation by default, ~~comprises an RSA signature verification instruction;~~ and

~~deploying, in the blockchain virtual machine,~~ RSA signature verification logic corresponding to the RSA signature verification instruction ~~is deployed in the~~
10 ~~blockchain virtual machine;~~

~~adding, to an instruction set of a smart contract compiler,~~ ~~comprises the RSA signature verification instruction;~~ and

~~generating, by using the a service smart contract compiler,~~ ~~compiled by using the a service smart contract compiler that comprises the RSA signature verification~~
15 ~~instruction;~~

~~deploying, in the blockchain network, the service smart contract that comprises the RSA signature verification instruction is deployed in a the blockchain network; and~~
 ~~the signature verification method comprises:~~

~~obtaining, by a node in the blockchain network, a service initiation transaction,~~
20 ~~and broadcasting the service initiation transaction to other nodes;~~

~~when executing the service initiation transaction,~~ invoking, by using the blockchain virtual machine ~~each node in the blockchain network,~~ the service smart contract ~~by using the blockchain virtual machine; and~~

triggering, by using the blockchain virtual machine ~~the node,~~ execution of the RSA
25 signature verification logic based on the RSA signature verification instruction in the service smart contract ~~by using the blockchain virtual machine,~~ to perform ~~an the~~ RSA signature verification operation on a service signature associated with a service initiation transaction that has been broadcasted to the blockchain network.

30 2. The method according to claim 1, wherein the service initiation transaction comprises the service signature, signed data corresponding to the service signature, and a public key used to verify the service signature; or

the service initiation transaction comprises the service signature, an abstract of signed data corresponding to the service signature, and a public key used to verify the service signature; or

the service initiation transaction comprises the service signature and signed data
5 corresponding to the service signature, and the service smart contract comprises a public key used to verify the service signature; or

the service initiation transaction comprises the service signature and an abstract of signed data corresponding to the service signature, and the service smart contract comprises a public key used to verify the service signature.

10

3. A blockchain smart contract-based signature verification method, wherein the method comprises:

adding, to an instruction set of a blockchain virtual machine that is associated with a blockchain network and that does not support an RSA signature verification
15 operation by default, comprises an RSA signature verification instruction; and

deploying, in the blockchain virtual machine, RSA signature verification logic corresponding to the RSA signature verification instruction ~~is deployed in the blockchain virtual machine;~~

adding, to an instruction set of a smart contract compiler, ~~comprises the RSA~~
20 ~~signature verification instruction;~~

generating, by using the a service smart contract compiler, compiled by using the a service smart contract compiler that comprises a contract identifier of an RSA signature verification smart contract, ~~and the RSA signature verification smart contract is a smart contract pre-deployed in a blockchain network;~~

25 deploying, in the blockchain network, the service smart contract that comprises the contract identifier of the RSA signature verification smart contract ~~is deployed in the blockchain network;~~ and

~~the signature verification method comprises:~~

~~obtaining, by a node in the blockchain network, a service initiation transaction;~~
30 ~~and broadcasting the service initiation transaction to other nodes;~~

~~when executing the service initiation transaction, invoking, by using the blockchain virtual machine each node in the blockchain network, the service smart contract by using the blockchain virtual machine;~~

invoking, by using the blockchain virtual machine~~the node~~, the RSA signature verification smart contract based on the contract identifier of the RSA signature verification smart contract in the service smart contract ~~by using the blockchain virtual machine~~; and

5 triggering, by using the blockchain virtual machine~~the node~~, execution of the RSA signature verification logic based on the RSA signature verification instruction in the RSA signature verification smart contract ~~by using the blockchain virtual machine~~, to perform ~~an~~ the RSA signature verification operation on a service signature associated with a service initiation transaction that has been broadcasted to the blockchain network.

10

4. A blockchain virtual machine, configured to implement the method according to any one of claims 1 to 3, wherein

~~an~~ the instruction set of the blockchain virtual machine comprises ~~an~~ the RSA signature verification instruction, and ~~a~~ the service smart contract compiled by using the smart contract compiler comprises the RSA signature verification instruction.

15

5. The blockchain virtual machine according to claim 4, wherein the instruction set of the blockchain virtual machine further comprises at least one Ethereum instruction, and the Ethereum instruction is an instruction in an instruction set of an Ethereum virtual machine; and

20

relevant logic corresponding to each Ethereum instruction comprised in the instruction set of the blockchain virtual machine is deployed in the blockchain virtual machine.

25 6. A smart contract compiler, configured to implement the method according to claim 1, wherein

~~an~~ the instruction set of the smart contract compiler comprises ~~an~~ the RSA signature verification instruction, and ~~a~~ the service smart contract compiled by using the smart contract compiler comprises the RSA signature verification instruction.

30

7. The smart contract compiler according to claim 6, wherein the instruction set of the smart contract compiler further comprises at least one Ethereum instruction, and the Ethereum instruction is an instruction in an instruction set of an Ethereum virtual machine.

8. A smart contract compiler, configured to implement the method according to claim 3, wherein

~~an~~the instruction set of the smart contract compiler comprises ~~an~~the RSA signature verification instruction, ~~a~~the service smart contract compiled by using the smart contract compiler comprises a contract identifier of an RSA signature verification smart contract, and the RSA signature verification smart contract is a smart contract pre-deployed in a blockchain network.

10 9. A blockchain system, comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform

15 operations comprising: a blockchain network, wherein

adding, to an instruction set of a blockchain virtual machine that is associated with a blockchain network and that does not support an RSA signature verification operation by default, comprises an RSA signature verification instruction;

deploying, in the blockchain virtual machine, RSA signature verification logic
20 corresponding to the RSA signature verification instruction~~is deployed in the blockchain virtual machine;~~

adding, to an instruction set of a smart contract compiler comprises the RSA signature verification instruction;

generating, by using the a service smart contract compiler, compiled by using the a service smart contract compiler that comprises the RSA signature verification instruction;
25 and

deploying, in the blockchain network, the service smart contract that comprises the RSA signature verification instruction~~is deployed in the blockchain network;~~

a node in the blockchain network obtains a service initiation transaction, and
30 broadcasts the service initiation transaction to other nodes; and

when executing the service initiation transaction, invoking, by using the blockchain virtual machine each node in the blockchain network, invokes the service smart contract by using the blockchain virtual machine; and

triggerings, by using the blockchain virtual machine, execution of the RSA signature verification logic based on the RSA signature verification instruction in the service smart contract ~~by using the blockchain virtual machine~~, to perform ~~an~~ the RSA signature verification operation on a service signature associated with a service
5 initiation transaction that has been broadcasted to the blockchain network.

10. A blockchain system, comprising:
one or more computers; and
one or more computer memory devices interoperably coupled with the one or
10 more computers and having tangible, non-transitory, machine-readable media storing
one or more instructions that, when executed by the one or more computers, perform
operations comprising: a blockchain network, wherein

adding, to an instruction set of a blockchain virtual machine that is associated
with a blockchain network and that does not support an RSA signature verification
15 operation by default, comprises an RSA signature verification instruction;

deploying, in the blockchain virtual machine, RSA signature verification logic
corresponding to the RSA signature verification instruction ~~is deployed in the~~
~~blockchain virtual machine;~~

adding, to an instruction set of a smart contract compiler, comprises the RSA
20 signature verification instruction;—

generating, by using the a service smart contract compiler, compiled by using the a
service smart contract compiler that comprises a contract identifier of an RSA signature
verification smart contract; ~~the RSA signature verification smart contract is a smart~~
~~contract pre-deployed in the blockchain network, and—~~

25 deploying, in the blockchain network, the service smart contract that comprises
the contract identifier of the RSA signature verification smart contract ~~is deployed in~~
~~the blockchain network;~~

~~a node in the blockchain network obtains a service initiation transaction, and~~
~~broadcasts the service initiation transaction to other nodes; and~~

30 ~~when executing the service initiation transaction, each~~ invoking, by using the
blockchain virtual machine node in the blockchain network, invokes the service smart
contract; ~~by using the blockchain virtual machine,—~~

invokinges, by using the blockchain virtual machine, the RSA signature
verification smart contract based on the contract identifier of the RSA signature

verification smart contract in the service smart contract ~~by using the blockchain virtual machine;~~ and

- 5 triggerings, by using the blockchain virtual machine, execution of the RSA signature verification logic based on the RSA signature verification instruction in the RSA signature verification smart contract ~~by using the blockchain virtual machine,~~ to perform the an RSA signature verification operation on a service signature associated with a service initiation transaction that has been broadcasted to the blockchain network.

- 10 11. A computer device, comprising a memory, a processor, and a computer program that is stored in the memory and that can run on the processor, wherein when executing the computer program, the processor implements the method according to any one of claims 1 to 3.