

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, an RSA signature verification instruction;

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

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

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

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

 invoking, by using the blockchain virtual machine, the service smart contract; and

 triggering, 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 to perform the RSA signature verification operation on a service
20 signature associated with a service initiation transaction that has been broadcasted to the blockchain network.

2. The method according to claim 1, wherein the service initiation transaction comprises the service signature, signed data corresponding to the service signature, and
25 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
30 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.

5 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 operation by default, an RSA signature verification instruction;

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

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

15 generating, by using the smart contract compiler, a service smart contract that comprises a contract identifier of an RSA signature verification smart contract;

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

invoking, by using the blockchain virtual machine, the service smart contract;

20 invoking, 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; and

25 triggering, 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, to perform the RSA signature verification operation on a service signature associated with a service initiation transaction that has been broadcasted to the blockchain network.

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

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

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

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

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

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

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

 the instruction set of the smart contract compiler comprises the RSA signature verification instruction, 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.

9. A blockchain system, comprising:

 one or more computers; and

30 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 operations comprising:

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, an RSA signature verification instruction;

5 deploying, in the blockchain virtual machine, RSA signature verification logic corresponding to the RSA signature verification instruction;

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

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

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

invoking, by using the blockchain virtual machine, the service smart contract; and

15 triggering, 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, to perform the RSA signature verification operation on a service signature associated with a service initiation transaction that has been broadcasted to the blockchain network.

10. A blockchain system, comprising:

20 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 operations comprising:

25 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, an RSA signature verification instruction;

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

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

generating, by using the smart contract compiler, a service smart contract that comprises a contract identifier of an RSA signature verification smart contract;

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

invoking, by using the blockchain virtual machine, the service smart contract;

5 invoking, 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; and

10 triggering, 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, to perform the RSA signature verification operation on a service signature associated with a service initiation transaction that has been broadcasted to the blockchain network.

11. A computer device, comprising a memory, a processor, and a computer
15 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.