

What is claimed is:

1. A computer-implemented method, comprising:

determining a first contract participant and a second contract participant of a plurality of contract participants in a blockchain;

generating, by each contract participant of the first and the second contract participants, respective temporary keys for a target contract, wherein the temporary keys generated by the first contract participant comprise a first temporary public key and a first temporary private key that are paired with each other, and the temporary keys generated by the second contract participant comprise a second temporary public key and a second temporary private key that are paired with each other, the temporary keys generated by the first contract participant being different from the temporary keys generated by the second contract participants;

sending, by the first contract participant, the first temporary public key to the second contract participant;

sending, by the second contract participant, the second temporary public key to the first contract participant;

signing, by each contract participant of the first and the second contract participants and by using a corresponding temporary private key generated by the contract participant, data information that comprises the target contract and temporary public keys of the other contract participant of the first and the second contract participants, to generate a respective first signature data corresponding to the contract participant signing the data information;

encrypting, the target contract and the respective first signature data of each contract participant of the first and the second contract participants by using a regulatory key of a regulator to generate encrypted data for the target contract;

determining that the first and the second contract participants reached a consensus offline on an execution process of the target contract;

in response to determining that the first and the second contract participants reached a consensus offline on the execution process of the target contract, encrypting, by a contract participant of the first and the second contract participants, a determined new contract by using the regulatory key, to generate an encrypted new contract;

signing, by each contract participant of the first and the second contract participants, the encrypted new contract by using a temporary private key corresponding to the encrypted new

contract, to generate a respective second signature data corresponding to each contract participant;

determining, by a contract participant of the first and the second contract participants, that the first and the second contract participants signed the encrypted new contract;

in response to determining that the first and the second contract participants signed the encrypted new contract, determining contract execution data comprising the respective second signature data of each contract participant ~~of the first and the second contract participants~~ and the encrypted new contract; and

submitting the ~~encrypted contract execution~~ data to the blockchain for storage as blockchain data, wherein the blockchain data comprises the contract execution data.

~~2. — The computer-implemented method of claim 1, comprising determining that the first and the second contract participants reached a consensus offline on an execution process of the target contract, wherein encrypting the new contract is performed in response to determining that the first and the second contract participants reached the consensus offline.~~

~~32.~~ The computer-implemented method of claim 1, further comprising:

sending, by each contract participant of the first and the second contract participants, digital identity digests of other contract participants of the first and the second contract participants to the blockchain;

receiving, by each contract participant of the first and the second contract participants, a message from the blockchain, wherein the message is an acknowledgement message or a failure message; and

in response to receiving the acknowledgement message from the blockchain, determining that the first and the second contract participants are legal users of the blockchain.

~~43.~~ The computer-implemented method of claim 1, wherein the temporary keys are updated based on:

at least one of different contract participants and different target contracts; or
a predetermined replacement period.

~~54.~~ The computer-implemented method of claim 1, wherein the target contract comprises certificates of all of the first and the second contract participants.

5. The computer-implemented method of claim 1, wherein the blockchain data comprises creation data.

6. The computer-implemented method of claim 1, further comprising:
performing a signature verification on the contract execution data by using temporary public keys corresponding to the encrypted new contract; and
in response to determining that the signature verification succeeds, updating the target contract to the encrypted new contract.

7. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

determining a first contract participant and a second contract participant of a plurality of contract participants in a blockchain;

generating, by each contract participant of the first and the second contract participants, respective temporary keys for a target contract, wherein the temporary keys generated by the first contract participant comprise a first temporary public key and a first temporary private key that are paired with each other, and the temporary keys generated by the second contract participant comprise a second temporary public key and a second temporary private key that are paired with each other, the temporary keys generated by the first contract participant being different from the temporary keys generated by the second contract participants;

sending, by the first contract participant, the first temporary public key to the second contract participant;

sending, by the second contract participant, the second temporary public key to the first contract participant;

signing, by each contract participant of the first and the second contract participants and by using a corresponding temporary private key generated by the contract participant, data information that comprises the target contract and temporary public keys of the other contract

participant of the first and the second contract participants, to generate a respective first signature data corresponding to the contract participant signing the data information;

encrypting, the target contract and the respective first signature data of each contract participant of the first and the second contract participants by using a regulatory key of a regulator to generate encrypted data for the target contract;

determining that the first and the second contract participants reached a consensus offline on an execution process of the target contract;

in response to determining that the first and the second contract participants reached a consensus offline on the execution process of the target contract, encrypting, by a contract participant of the first and the second contract participants, a determined new contract by using the regulatory key, to generate an encrypted new contract;

signing, by each contract participant of the first and the second contract participants, the encrypted new contract by using a temporary private key corresponding to the encrypted new contract, to generate a respective second signature data corresponding to each contract participant;

determining, by a contract participant of the first and the second contract participants, that the first and the second contract participants signed the encrypted new contract;

in response to determining that the first and the second contract participants signed the encrypted new contract, determining contract execution data comprising the respective second signature data of each contract participant ~~of the first and the second contract participants~~ and the encrypted new contract; and

submitting the ~~contract execution~~encrypted data to the blockchain for storage as blockchain data, wherein the blockchain data comprises the contract execution data.

~~8.——The computer-readable medium of claim 7, wherein the operations further comprise determining that the first and the second contract participants reached a consensus offline on an execution process of the target contract, wherein encrypting the new contract is performed in response to determining that the first and the second contract participants reached the consensus offline.~~

98. The computer-readable medium of claim 7, wherein the operations further comprise:

sending, by each contract participant of the first and the second contract participants, digital identity digests of other contract participants of the first and the second contract participants to the blockchain;

receiving, by each contract participant of the first and the second contract participants, a message from the blockchain, wherein the message is an acknowledgement message or a failure message; and

in response to receiving the acknowledgement message from the blockchain, determining that the first and the second contract participants are legal users of the blockchain.

~~109.~~ The computer-readable medium of claim 7, wherein the temporary keys are updated based on:

at least one of different contract participants and different target contracts; or
a predetermined replacement period.

~~110.~~ The computer-readable medium of claim 7, wherein the target contract comprises certificates of all of the first and the second contract participants.

11. The computer-readable medium of claim 7, wherein the blockchain data comprises creation data.

12. The computer-readable medium of claim 7, wherein the operations further comprise:
performing a signature verification on the contract execution data by using temporary public keys corresponding to the encrypted new contract; and

in response to determining that the signature verification succeeds, updating the target contract to the encrypted new contract.

13. A computer-implemented 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, cause the one or more computers to perform one or more operations comprising:

determining a first contract participant and a second contract participant of a plurality of contract participants in a blockchain;

generating, by each contract participant of the first and the second contract participants, respective temporary keys for a target contract, wherein the temporary keys generated by the first contract participant comprise a first temporary public key and a first temporary private key that are paired with each other, and the temporary keys generated by the second contract participant comprise a second temporary public key and a second temporary private key that are paired with each other, the temporary keys generated by the first contract participant being different from the temporary keys generated by the second contract participants;

sending, by the first contract participant, the first temporary public key to the second contract participant;

sending, by the second contract participant, the second temporary public key to the first contract participant;

signing, by each contract participant of the first and the second contract participants and by using a corresponding temporary private key generated by the contract participant, data information that comprises the target contract and temporary public keys of the other contract participant of the first and the second contract participants, to generate a respective first signature data corresponding to the contract participant signing the data information;

encrypting, the target contract and the respective first signature data of each contract participant of the first and the second contract participants by using a regulatory key of a regulator to generate encrypted data for the target contract;

determining that the first and the second contract participants reached a consensus offline on an execution process of the target contract;

in response to determining that the first and the second contract participants reached a consensus offline on the execution process of the target contract, encrypting, by a contract participant of the first and the second contract participants, a determined new contract by using the regulatory key, to generate an encrypted new contract;

signing, by each contract participant of the first and the second contract participants, the encrypted new contract by using a temporary private key corresponding to the encrypted new

contract, to generate a respective second signature data corresponding to each contract participant;

determining, by a contract participant of the first and the second contract participants, that the first and the second contract participants signed the encrypted new contract;

in response to determining that the first and the second contract participants signed the encrypted new contract, determining contract execution data comprising the respective second signature data of each contract participant ~~of the first and the second contract participants~~ and the encrypted new contract; and

submitting the ~~contract execution encrypted~~ data to the blockchain for storage as blockchain data, wherein the blockchain data comprises the contract execution data.

~~14. The computer-implemented system of claim 13, wherein the operations further comprise determining that the first and the second contract participants reached a consensus offline on an execution process of the target contract, wherein encrypting the new contract is performed in response to determining that the first and the second contract participants reached the consensus offline.~~

~~15~~14. The computer-implemented system of claim 13, wherein the operations further comprise:

sending, by each contract participant of the first and the second contract participants, digital identity digests of other contract participants of the first and the second contract participants to the blockchain;

receiving, by each contract participant of the first and the second contract participants, a message from the blockchain, wherein the message is an acknowledgement message or a failure message; and

in response to receiving the acknowledgement message from the blockchain, determining that the first and the second contract participants are legal users of the blockchain.

~~16~~15. The computer-implemented system of claim 13, wherein the temporary keys are updated based on:

at least one of different contract participants and different target contracts; or
a predetermined replacement period.

~~17~~16. The computer-implemented system of claim 13, wherein the target contract comprises certificates of all of the first and the second contract participants.

~~18~~17. The computer-implemented system of claim 13, wherein the blockchain data comprises creation data ~~operations further comprise:~~

~~———performing a signature verification on the contract execution data by using temporary public keys corresponding to the encrypted new contract; and~~

~~in response to determining that the signature verification succeeds, updating the target contract to the encrypted new contract.~~