CLAIMS

What is claimed is:

1. A data processing method based on an intelligent contract, performed by an electronic device as a contract node, the method comprising:

receiving a firmware update request corresponding to a first server node transmitted by an execution node, the firmware update request comprising at least an updated version parameter of the first server node;

invoking an intelligent contract according to the firmware update request, and obtaining, from a blockchain based on the intelligent contract, a firmware version update record and a firmware version release record that are associated with the first server node, the firmware version release record being determined by a release node on the blockchain based on a consensus mechanism, wherein the release node is configured to receive a latest version firmware file released for a firmware in the first server node; and

determining validity of the firmware update request according to the firmware version update record, the firmware version release record, and the updated version parameter.

2. The method according to claim 1, wherein the invoking an intelligent contract, and obtaining, from a blockchain, a firmware version update record and a firmware version release record that are associated with the first server node comprises:

invoking the intelligent contract to obtain a blockchain address of the first server node in the blockchain, the blockchain address being uniquely determined by the blockchain after hash calculation is performed according to public key information of the first server node;

obtaining, based on the blockchain address from the blockchain, a first block and a second block that are associated with the first server node;

determining historical version update behavior information from the first block as the firmware version update record associated with the first server node, the historical version update behavior information carrying a first version parameter and a second version parameter, and the second version parameter being a version parameter obtained after firmware update is performed on the first version parameter; and

determining historical version release behavior information associated with the first server node from the second block as the firmware version release record.

3. The method according to claim 2, wherein the determining validity of the firmware update request according to the firmware version update record, the firmware version release record, and the updated version parameter comprises:

performing rollback detection on the updated version parameter based on the first version parameter in the firmware version update record;

determining, in response to detecting that the first version parameter is the same as the updated version parameter, that version rollback exists, and determining that the firmware update request is an invalid update request, the invalid update request being used for indicating that the execution node does not have permission to perform firmware update on version information of the first server node; and

determining, in response to detecting that the first version parameter is different from the updated version parameter, that the version rollback does not exist, and determining the validity of the firmware update request based on the updated version parameter and the firmware version release record.

4. The method according to claim 3, wherein the determining that the firmware update request is a valid update request based on the updated version parameter and the firmware version release record comprises:

obtaining first version release behavior information from the historical version release behavior information associated with the firmware version release record, the first version release behavior information being version release behavior information having a maximum version release timestamp in the historical version release behavior information; and

determining that the firmware update request is the valid update request in response to detecting that the first version release behavior information comprises the updated version parameter.

5. The method according to claim 4, wherein the firmware update request further comprises a running version parameter of the first server node; and

the method further comprises:

searching, in response to detecting that the first version release behavior information does not comprise the updated version parameter, and second version release behavior information in the historical version release behavior information comprises the updated version parameter, the blockchain for M second server nodes on which firmware update is performed by using the updated version parameter, M being a positive integer greater than 2;

obtaining version update behavior information of the M second server nodes;

determining that the firmware update request is the valid update request in response to detecting that the version update behavior information of the M second server nodes comprises the running version parameter; and

determining that the firmware update request is the invalid update request in response to detecting that version update behavior information that does not comprise the running version parameter exists in the version update behavior information of the M second server nodes.

6. The method according to claim 5, further comprising:

returning to the execution node, in response to determining that the firmware update request is the valid update request, feedback information used for performing firmware update on the first server node, the feedback information being used for instructing the execution node to update firmware version information of the first server node from running version information in the running version parameter to updated version information in the updated version parameter.

7. The method according to claim 5, further comprising:

determining, in response to detecting that the firmware update request is the invalid update request, that execution of a contract fails, and returning the invalid update request to the execution node; and

identifying, when a next firmware update request corresponding to the first server node transmitted by the execution node is received, the next firmware update request as the invalid update request, the invalid update request being used for instructing the release node to generate alarm information for the execution node during security audit.

8. The method according to claim 7, wherein the alarm information is obtained by the release node after the security audit is performed according to an on-chain updated version parameter of the first server obtained from the blockchain and an updated running version parameter locally acquired from the first server node.

9. The method according to claim 1, further comprising:

receiving confirmation information after the first server node signs the updated version parameter, the confirmation information indicating that the execution node has updated firmware version information of the first server node;

performing signature verification on the confirmation information by using public key information of the first server node, determining, when the signature verification succeeds, that the

invoking of the intelligent contract is completed; and

updating the firmware version update record of the first server node based on the confirmation information and the firmware update request, and writing an updated firmware version update record into the blockchain based on a blockchain address of the first server node.

10. The method according to claim 9, wherein the updating the firmware version update record of the first server node based on the confirmation information and the firmware update request, and writing an updated firmware version update record into the blockchain based on a blockchain address of the first server node comprises:

using the updated version parameter and a running version parameter in the firmware update request as input information for constructing the firmware version update record associated with the first server node;

using the updated version parameter carried in the confirmation information as output information for constructing the firmware version update record associated with the first server node;

determining, based on the input information and the output information, target version update behavior information associated with the first server node, and updating the firmware version update record of the first server node based on the target version update behavior information; and

writing the updated firmware version update record into the blockchain based on the blockchain address of the first server node.

11. A data processing apparatus based on an intelligent contract, applied to a contract node, and the apparatus comprising:

a request receiving module, configured to receive a firmware update request corresponding to a first server node transmitted by an execution node, the firmware update request comprising at least an updated version parameter of the first server node;

a contract invoking module, configured to invoke an intelligent contract according to the firmware update request, and obtain, from a blockchain based on the intelligent contract, a firmware version update record and a firmware version release record that are associated with the first server node, the firmware version release record being determined by a release node on the blockchain based on a consensus mechanism, wherein the release node is configured to receive a latest version firmware file released for a firmware in the first server node; and

a validity determining module, configured to determine validity of the firmware update request

according to the firmware version update record, the firmware version release record, and the updated version parameter.

12. The apparatus according to claim 11, wherein the contract invoking module comprises:

an address obtaining unit, configured to invoke the intelligent contract to obtain a blockchain address of the first server node in the blockchain, the blockchain address being uniquely determined by the blockchain after hash calculation is performed according to public key information of the first server node;

a block obtaining unit, configured to obtain, based on the blockchain address from the blockchain, a first block and a second block that are associated with the first server node;

an update record determining unit, configured to determine historical version update behavior information from the first block as the firmware version update record associated with the first server node, the historical version update behavior information carrying a first version parameter and a second version parameter, and the second version parameter being a version parameter obtained after firmware update is performed on the first version parameter; and

a release record determining unit, configured to determine historical version release behavior information associated with the first server node from the second block as the firmware version release record.

13. The apparatus according to claim 12, wherein the validity determining module comprises:

a rollback detection unit, configured to perform rollback detection on the updated version parameter based on the first version parameter in the firmware version update record;

an invalidity determining unit, configured to determine, in response to detecting that the first version parameter is the same as the updated version parameter, that version rollback exists, and the firmware update request is an invalid update request, the invalid update request being used for indicating that the execution node does not have permission to perform firmware update on version information of the first server node; and

a validity determining unit, configured to determine, in response to detecting that the first version parameter is different from the updated version parameter, that the version rollback does not exist, and determine the validity of the firmware update request based on the updated version parameter and the firmware version release record.

14. A node device, comprising a processor and a memory,

the processor being connected to the memory, the memory being configured to store program

code, and the processor being configured to invoke the program code to perform the method according to any one of claims 1 to 10.

15. A computer storage medium, storing a computer program, the computer program comprising program instructions, the program instructions, when executed by a processor, causing the method according to any one of claims 1 to 10 to be performed.