CLAIMS

1. A computer-implemented method for asset management, the computer-implemented method comprising:

receiving, from a target user having an account recorded in a distributed database of a blockchain network, a user input comprising a request to update a status of a target object that was transferred among a plurality of holders, the request being signed by the target user using a private key;

determining a contract object associated with the target object, the contract object being published in the blockchain network and corresponding to an asset type of the target object, wherein the target object was created using the contract object, and wherein the contract object comprises a list of member users with an update permission for the target object and information about public keys held by the member users;

performing an identity authentication of the target user based on a respective public key corresponding to the private key used for signing the request;

in response to a successful identity authentication of the target user, determining, based on the contract object, that the target user is a current holder of the target object and is included in the list of member users with the update permission for the target object; and

in response to determining that the target user has the update permission for the target object, performing a status update on the target object by invoking the contract object.

2. The computer-implemented method of claim 1, wherein performing the identity authentication of the target user comprises executing an authentication program corresponding to the update permission for the target object.

3. The computer-implemented method of claim 1, wherein the contract object comprises a whitelist of target objects authorized to hold an asset object created by invoking the contract object.

4. The computer-implemented method of claim 1, wherein the contract object comprises a code field that is used to maintain an execution code related to an execution program.

5. The computer-implemented method of claim 1, wherein the blockchain network comprises a consortium chain, and the target user in the blockchain network is a consortium member that has asset object generation authority in the consortium chain.

6. The computer-implemented method of claim 1, wherein the status of the target object comprises a flag indicating a performance of the target user.

7. The computer-implemented method of claim 1, further comprising generating for the target user a public key associated with an account address of an institution in the blockchain network and a private key configured to be used by the institution to operate an account corresponding to the account address.

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

receiving, from a target user having an account recorded in a distributed database of a blockchain network, a user input comprising a request to update a status of a target object that was transferred among a plurality of holders, the request being signed by the target user using a private key;

determining a contract object associated with the target object, the contract object being published in the blockchain network and corresponding to an asset type of the target object, wherein the target object was created using the contract object, and wherein the contract object comprises a list of member users with an update permission for the target object and information about public keys held by the member users;

performing an identity authentication of the target user based on a respective public key corresponding to the private key used for signing the request;

in response to a successful identity authentication of the target user, determining, based on the contract object, that the target user is a current holder of the target object and is included in the list of member users with the update permission for the target object; and

in response to determining that the target user has the update permission for the target object, performing a status update on the target object by invoking the contract object.

9. The non-transitory, computer-readable medium of claim 8, wherein performing the identity authentication of the target user comprises executing an authentication program corresponding to the update permission for the target object.

10. The non-transitory, computer-readable medium of claim 8, wherein the contract object comprises a whitelist of target objects authorized to hold an asset object created by invoking the contract object.

11. The non-transitory, computer-readable medium of claim 8, wherein the contract object comprises a code field that is used to maintain an execution code related to an execution program.

12. The non-transitory, computer-readable medium of claim 8, wherein the blockchain network comprises a consortium chain, and the target user in the blockchain network is a consortium member that has asset object generation authority in the consortium chain.

13. The non-transitory, computer-readable medium of claim 8, wherein the status of the target object comprises a flag indicating a performance of the target user.

14. The non-transitory, computer-readable medium of claim 8, wherein the operations further comprise generating for the target user a public key associated with an account address of an institution in the blockchain network and a private key configured to be used by the institution to operate an account corresponding to the account address.

15. 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, perform operations comprising:

receiving, from a target user having an account recorded in a distributed database of a blockchain network, a user input comprising a request to update a status of a target object that was transferred among a plurality of holders, the request being signed by the target user using a private key;

determining a contract object associated with the target object, the contract object being published in the blockchain network and corresponding to an asset type of the target object, wherein the target object was created using the contract object, and

wherein the contract object comprises a list of member users with an update permission for the target object and information about public keys held by the member users;

performing an identity authentication of the target user based on a respective public key corresponding to the private key used for signing the request;

in response to a successful identity authentication of the target user, determining, based on the contract object, that the target user is a current holder of the target object and is included in the list of member users with the update permission for the target object; and

in response to determining that the target user has the update permission for the target object, performing a status update on the target object by invoking the contract object.

16. The computer-implemented system of claim 15, wherein performing the identity authentication of the target user comprises executing an authentication program corresponding to the update permission for the target object.

17. The computer-implemented system of claim 15, wherein the contract object comprises a whitelist of target objects authorized to hold an asset object created by invoking the contract object.

18. The computer-implemented system of claim 15, wherein the contract object comprises a code field that is used to maintain an execution code related to an execution program.

19. The computer-implemented system of claim 15, wherein the blockchain network comprises a consortium chain, and the target user in the blockchain network is a consortium member that has asset object generation authority in the consortium chain.

20. The computer-implemented system of claim 15, wherein the status of the target object comprises a flag indicating a performance of the target user.