

CLAIMS

What is claimed is:

1. A method for asset management, the method comprising:
receiving, by a node device in a blockchain, a status update request initiated by a target user for a target asset object (102);
in response to the status update request, verifying whether the target user is a member user with update permission for the target asset object in a smart contract object that is published in the blockchain and corresponds to an asset type of the target asset object, wherein the target asset object is created by invoking the smart contract object (104); and
performing a status update on the target asset object by invoking the smart contract object if the target user is a member user with update permission for the target asset object in the smart contract object (106).
2. The method according to claim 1, wherein an authentication program corresponding to the update permission for the target asset object is stated in the smart contract object.
3. The method according to claim 2, wherein verifying whether the target user is a member user with update permission for the target asset object in a smart contract object that is published in the blockchain and corresponds to an asset type of the target asset object comprises:
performing permission authentication on the target user by invoking the authentication program stated in the smart contract object corresponding to the asset type of the target asset object, and determining that the target user is a member user with update permission for the target asset object if permission authentication succeeds.
4. The method according to claim 1, wherein a user list of member users with update permission for the target asset object is stated in the smart contract object.

5. The method according to claim 4, wherein verifying whether the target user is a member user with update permission for the target asset object in a smart contract object that is published in the blockchain and corresponds to an asset type of the target asset object comprises:

verifying whether the target user matches a member user in the user list, and determining that the target user is a member user with update permission for the target asset object if the target user matches a member user in the user list.

6. The method according to claim 3, wherein the user list is a public key list of the member users with update permission for the target asset object, and the status update request is signed by the target user based on a held private key.

7. The method according to claim 6, wherein verifying whether the target user matches the member user in the user list comprises:

performing authentication on a signature of the status update request based on a public key in the public key list, and determining that the target user matches a member user in the user list if authentication succeeds.

8. The method according to claim 1, wherein an execution program used to perform the status update on the target asset object is stated in the smart contract object.

9. The method according to claim 8, wherein performing the status update on the target asset object by invoking the smart contract object comprises:

performing the status update on the target asset object by invoking the execution program stated in the smart contract object.

10. The method according to claim 9, wherein objects supported by the blockchain comprise an account object, a smart contract object, and an asset object, the object supported by the blockchain comprises a status field, and the status field is used to maintain status information of the object.

11. The method according to claim 10, wherein performing the status update on the target asset object by invoking the execution program stated in the smart contract object comprises:
performing a status update on the target asset object by invoking the execution program stated in the smart contract object and adding status information of the target asset object that is comprised in the status update request to a status field in the target asset object.
12. The method according to claim 11, wherein the object supported by the blockchain further comprises a code field, and the code field is used to maintain execution code related to an execution program stated in the object.
13. The method according to claim 1, wherein the blockchain is a consortium blockchain, and a target member in the blockchain is a consortium member with asset object creation permission in the consortium blockchain.
14. The method according to claim 1, further comprising:
in response to the status update request, verifying whether the target user is a publisher of a smart contract object that is published in the blockchain and corresponds to an asset type of the target asset object, wherein the target asset object is created by invoking the smart contract object; and
performing a status update on the target asset object by invoking the smart contract object if the target user is a member user who publishes the smart contract object.
15. An apparatus for asset management, the apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 14.