

CLAIMS:

1. A computer-implemented method for updating data in blockchain, to be performed by a system for updating data in blockchain, comprising:

obtaining, from a client, one or more requests for updating a plurality of pieces of data in one or more blockchains, wherein the client corresponds to one or more local accounts in the system, and the one or more requests comprise one or more unsigned blockchain transactions;

obtaining one or more blockchain addresses respectively associated with the one or more local accounts and obtaining one or more private keys respectively associated with the one or more blockchain addresses; and

updating the plurality of pieces of data in the one or more blockchains based at least on the one or more blockchain addresses and the one or more private keys by:

updating the one or more unsigned blockchain transactions respectively based on the one or more blockchain addresses,

signing, in a Trusted Execution Environment (TEE), the one or more updated blockchain transactions respectively with the one or more private keys, and

transmitting the signed one or more blockchain transactions to one or more blockchain nodes of the one or more blockchains for execution, wherein:

the one or more blockchain addresses and the one or more private keys are stored in the system and are not stored at the client.

2. The method of claim 1, wherein:

obtaining the one or more requests for updating the plurality of pieces of data in the one or more blockchains comprises: obtaining the one or more requests for updating the plurality of pieces of data respectively in a plurality of blockchains in association with one local account; and

updating the plurality of pieces of data of the one or more blockchains comprises: respectively in the plurality of blockchains, updating in a batch the plurality of pieces of data.

3. The method of claim 1, wherein:

obtaining the one or more requests for updating the plurality of pieces of data in the one or more blockchains comprises: obtaining the one or more requests for updating the plurality of pieces of data in one blockchain respectively in association with a plurality of local accounts; and

updating the plurality of pieces of data of the one or more blockchains comprises: in the one blockchain, updating in a batch the plurality of pieces of data.

4. The method of claim 1, wherein:

obtaining the one or more requests for updating the plurality of pieces of data in the one or more blockchains comprises: obtaining the one or more requests for updating the plurality of pieces of data respectively in a plurality of blockchains in association with a plurality of local accounts; and

updating the plurality of pieces of data of the one or more blockchains comprises: respectively in the plurality of blockchains, updating in a batch the plurality pieces of data.

5. The method of claim 1, wherein:

obtaining the one or more requests for updating the plurality of pieces of data in the one or more blockchains comprises: obtaining the one or more local accounts, the one or more unsigned blockchain transactions, information of the plurality of pieces of data, and one or more identifications of the one or more blockchains corresponding to the one or more blockchain transactions; and

the information of the plurality of pieces of data comprises: new data to add to the one or more blockchains or changes to make to existing data in the one or more blockchains.

6. The method of claim 1, wherein transmitting the signed one or more blockchain transactions to one or more blockchain nodes for execution comprises:

constructing a master blockchain transaction comprising the signed one or more blockchain transactions; and

sending the master blockchain transaction to the one or more blockchain nodes of the one or more blockchains according to the one or more identifications of the one or more blockchains for execution.

7. The method of claim 1, wherein:

obtaining the one or more private keys respectively associated with the one or more blockchain addresses comprises: retrieving the one or more private keys in an encrypted form;

updating the one or more unsigned blockchain transactions respectively based on the one or more blockchain addresses comprises: adding the one or more blockchain addresses respectively to the one or more unsigned blockchain transactions; and

signing the one or more updated blockchain transactions respectively with the one or more private keys comprises: decrypting the retrieved one or more private keys in the encrypted form and signing the one or more updated blockchain transactions respectively with the one or more private keys in a decrypted form.

8. The method of claim 7, wherein:

retrieving the one or more private keys in the encrypted form comprises: retrieving the one or more private keys in the encrypted form from a Key Management System (KMS) according to one or more KMS directories in one or more mapping relationships;

the one or more mapping relationships associate the one or more local accounts with the one or more blockchain addresses and the one or more KMS directories; and

the one or more KMS directories link to the one or more private keys in the encrypted form.

9. The method of claim 1, wherein:

obtaining the one or more requests for updating the plurality of pieces of data in the one or more blockchains comprises: obtaining, from the client, the one or more requests for updating the plurality of pieces of data in the one or more blockchains in accordance with a Lightweight Directory Access Protocol (LDAP).

10. A system for updating data in blockchain, comprising one or more processors and one or more non-transitory computer-readable memories coupled to the one or more processors and configured with instructions executable by the one or more processors to cause the system to perform operations comprising:

obtaining, from a client, one or more requests for updating a plurality of pieces of data in one or more blockchains, wherein the client corresponds to one or more local accounts in the system, and the one or more requests comprise one or more unsigned blockchain transactions;

obtaining one or more blockchain addresses respectively associated with the one or more local accounts and obtaining one or more private keys respectively associated with the one or more blockchain addresses; and

updating the plurality of pieces of data in the one or more blockchains based at least on the one or more blockchain addresses and the one or more private keys by:

updating the one or more unsigned blockchain transactions respectively based on the one or more blockchain addresses,

signing, in a Trusted Execution Environment (TEE), the one or more updated blockchain transactions respectively with the one or more private keys, and

transmitting the signed one or more blockchain transactions to one or more blockchain nodes of the one or more blockchains for execution, wherein:

the one or more blockchain addresses and the one or more private keys are stored in the system and are not stored at the client.

11. The system of claim 10, wherein:

obtaining the one or more requests for updating the plurality of pieces of data in the one or more blockchains comprises: obtaining the one or more local accounts, the one or more unsigned blockchain transactions, information of the plurality of pieces of data, and one or more identifications of the one or more blockchains corresponding to the one or more blockchain transactions; and

the information of the plurality of pieces of data comprises: new data to add to the one or more blockchains or changes to make to existing data in the one or more blockchains.

12. The system of claim 10, wherein:

obtaining the one or more requests for updating the plurality of pieces of data in the one or more blockchains comprises: obtaining the one or more requests for updating the plurality of pieces of data respectively in a plurality of blockchains in association with a plurality of local accounts; and

updating the plurality of pieces of data of the one or more blockchains comprises: respectively in the plurality of blockchains, updating in a batch the plurality pieces of data.

13. The system of claim 10, wherein transmitting the signed one or more blockchain transactions to one or more blockchain nodes for execution comprises:

constructing a master blockchain transaction comprising the signed one or more blockchain transactions; and

sending the master blockchain transaction to the one or more blockchain nodes of the one or more blockchains according to the one or more identifications of the one or more blockchains for execution.

14. A non-transitory computer-readable storage medium for updating data in blockchain, the storage medium associated with a system for updating data in blockchain, the storage

medium configured with instructions executable by one or more processors to cause the one or more processors to perform operations comprising:

- obtaining, from a client, one or more requests for updating a plurality of pieces of data in one or more blockchains, wherein the client corresponds to one or more local accounts in the system, and the one or more requests comprise one or more unsigned blockchain transactions;

- obtaining one or more blockchain addresses respectively associated with the one or more local accounts and obtaining one or more private keys respectively associated with the one or more blockchain addresses; and

- updating the plurality of pieces of data in the one or more blockchains based at least on the one or more blockchain addresses and the one or more private keys by:

 - updating the one or more unsigned blockchain transactions respectively based on the one or more blockchain addresses,

 - signing, in a Trusted Execution Environment (TEE), the one or more updated blockchain transactions respectively with the one or more private keys, and

 - transmitting the signed one or more blockchain transactions to one or more blockchain nodes of the one or more blockchains for execution, wherein:

 - the one or more blockchain addresses and the one or more private keys are stored in the system and are not stored at the client.

15. The storage medium of claim 14, wherein:

- obtaining the one or more requests for updating the plurality of pieces of data in the one or more blockchains comprises: obtaining the one or more local accounts, the one or more unsigned blockchain transactions, information of the plurality of pieces of data, and one or more identifications of the one or more blockchains corresponding to the one or more blockchain transactions; and

 - the information of the plurality of pieces of data comprises: new data to add to the one or more blockchains or changes to make to existing data in the one or more blockchains.

16. The storage medium of claim 14, wherein:

- obtaining the one or more requests for updating the plurality of pieces of data in the one or more blockchains comprises: obtaining the one or more requests for updating the plurality of pieces of data respectively in a plurality of blockchains in association with one local account; and

updating the plurality of pieces of data of the one or more blockchains comprises: respectively in the plurality of blockchains, updating in a batch the plurality of pieces of data.

17. The storage medium of claim 14, wherein transmitting the signed one or more blockchain transactions to one or more blockchain nodes for execution comprises:

constructing a master blockchain transaction comprising the signed one or more blockchain transactions; and

sending the master blockchain transaction to the one or more blockchain nodes of the one or more blockchains according to the one or more identifications of the one or more blockchains for execution.

18. The storage medium of claim 14, wherein:

obtaining the one or more requests for updating the plurality of pieces of data in the one or more blockchains comprises: obtaining the one or more requests for updating the plurality of pieces of data in one blockchain respectively in association with a plurality of local accounts; and

updating the plurality of pieces of data of the one or more blockchains comprises: in the one blockchain, updating in a batch the plurality of pieces of data.