

CLAIMS

What is claimed is:

1. A method for performing non-custodial authentication for a client, comprising:
generating a private key by the client, the client associated with a user;
generating, at the client, a decentralized identifier token (DIDT) from the private key;
and
authenticating the user for an application based on the DIDT.
2. The method of claim 1, further comprising:
receiving an access token from a remote service by a client from a server; and
receiving scoped credentials from the remote service based on the access token, the
scoped credentials providing client authorization to the third service.
3. The method of claim 2, further comprising
accessing an encrypted copy of the private key;
providing the encrypted copy of the private key and the scoped credentials to the
remote service; and
receiving the decrypted private key by the client from the remote service.
4. The method of claim 3, further comprising:
wherein a hardware security module in communication with the third-party service
decrypts and encrypts the private key.
5. The method of claim 4, wherein the hardware security module decrypts and encrypts
the private key using a master key that cannot be exported by the remote service.
6. The method of claim 2, further comprising:

transmitting the generated private key and scoped credentials to a remote hardware security module; and

receiving an encrypted private key from the hardware security module.

7. The method of claim 1, further comprising:
 - receiving a message from the client by the server, the message identifying a user at the client;
 - registering the user with the third-party service;
 - receiving the access token by the server from the third-party service in response to registering the user with the third-party service; and
 - transmitting the access token to the client by the server.
8. The method of claim 1, further comprising uploading the encrypted private key from the client to the server.
9. The method of claim 1, wherein the client includes a network browser, the network browser providing an iframe, the private key generated by code within the iframe, wherein the DIDT is generated by code executing within the iframe of the network browser.
10. The method of claim 8, further comprising:
 - detecting a lost password event from the client;
 - providing a second access token to the client by the server;
 - accessing scoped credentials based on the access token by the client;
 - transmitting the scoped credentials and the encrypted key to the remote service; and
 - receiving a decrypted copy of the private key by the client based at least in part on the scoped credentials.
11. The method of claim 1, further comprising:
 - signing transaction data based on the encrypted private key; and

submitting the transaction data to be stored at a plurality of linked peer-to-peer computers that store data in blocks that are linked together.

12. A non-transitory computer readable storage medium having embodied thereon a program, the program being executable by a processor to perform a method for method for performing non-custodial authentication for a client, the method comprising
generating a private key by the client, the client associated with a user;
generating, at the client, a decentralized identifier token (DIDT) from the private key;
and
authenticating the user for an application based on the DIDT.
13. The method of claim 1, further comprising:
receiving an access token from a remote service by a client from a server; and
receiving scoped credentials from the remote service based on the access token, the scoped credentials providing client authorization to the third service.
14. The method of claim 2, further comprising
accessing an encrypted copy of the private key;
providing the encrypted copy of the private key and the scoped credentials to the remote service; and
receiving the decrypted private key by the client from the remote service.
15. The method of claim 2, further comprising:
transmitting the generated private key and scoped credentials to a remote hardware security module; and
receiving an encrypted private key from the hardware security module.
16. The method of claim 1, further comprising:

receiving a message from the client by the server, the message identifying a user at the client;

registering the user with the third-party service;

receiving the access token by the server from the third-party service in response to registering the user with the third-party service; and

transmitting the access token to the client by the server.

17. The method of claim 1, further comprising uploading the encrypted private key from the client to the server.

18. The method of claim 1, wherein the client includes a network browser, the network browser providing an iframe, the private key generated by code within the iframe, wherein the DIDT is generated by code executing within the iframe of the network browser.

19. The method of claim 8, further comprising:

detecting a lost password event from the client;

providing a second access token to the client by the server;

accessing scoped credentials based on the access token by the client;

transmitting the scoped credentials and the encrypted key to the remote service; and

receiving a decrypted copy of the private key by the client based at least in part on the scoped credentials.

20. A system for performing non-custodial authentication for a client, the system comprising:

a server including a memory and a processor; and

one or more modules stored in the memory and executed by the processor to:

providing an access token for a remote service to a client from a server,

receiving scoped credentials from the third-party service based on the access token, and

authenticating the user based on the scoped credentials.