

Claims

1. A method to setup a wallet for a decentralized application by performing non-custodial authentication for a client, comprising: sending, over a network by the client to an authentication server, a sign-up request for a user account associated with the decentralized application; receiving over the network at the client from the authentication server, an access token that corresponds to the sign-up request, for use at a third party key storage server; generating a key by the client; and sending over the network from the client to the third party key storage server and bypassing the authentication server, one or more messages that include the access token, the key, and a request to encrypt the key.
2. The method of claim 1, wherein sending the sign-up request includes sending first authentication information over the network from the client to the authentication server.
3. The method of claim 1, further including: receiving a request for first authentication information over the network at the client based on the sign-up request.
4. The method of claim 3, wherein receiving the request for first authentication information over the network at the client based on the sign-up request includes receiving an email at the client from the authentication server or receiving a message at a phone number associated with the client from the authentication system.
5. The method of claim 1, wherein requesting sign-up includes sending a login request.
6. The method of claim 1, wherein generating the key includes generating a public-private key pair.
7. The method of claim 1, wherein receiving the access token includes receiving an access token that is generated at the third party key storage server.
8. The method of claim 1, wherein sending the one or more messages over the network from the client to the third party key storage server and bypassing the authentication server includes sending an authentication credential from the client to the third party key storage server.
9. The method of claim 8 further including: receiving the authentication credential from the third party key storage server.

10. The method of claim 9, wherein sending the one or more messages over the network from the client to the third party key storage server and bypassing the authentication server includes sending the access token to the third party key storage server followed by sending the authentication credential, the key, and the request to encrypt the key from the client to the third party key storage server.

11. A non-transitory computer readable storage medium having embodied thereon a program, the program being executable by a processor to perform a method to setup a wallet for a decentralized application by performing a non-custodial authentication method for a client, the method comprising: sending, over a network by the client to an authentication system, a sign-up request for a user account associated with the decentralized application; receiving over the network at the client from the authentication system, an access token that corresponds to the sign-up request, for use at a third party key storage system; generating a key by the client; and sending over the network from the client to the third party key storage system and bypassing the authentication system, one or more messages that include the access token, the key, and a request to encrypt the key.

12. The non-transitory computer readable storage medium of claim 11, further including: sending authentication information over the network from the client to the authentication system.

13. The non-transitory computer readable storage medium of claim 11 further including: receiving a request for authentication information over the network at the client based on the sign-up request.

14. The non-transitory computer readable storage medium of claim 13, wherein receiving the request for authentication information over the network at the client based on the sign-up request includes receiving an email at the client from the authentication system or receiving a message at a phone number associated with the client from the authentication system.

15. The non-transitory computer readable storage medium of claim 11, wherein requesting sign-up includes sending a login request.

16. The method of claim 11, wherein generating the key includes generating a public-private key pair.

17. The non-transitory computer readable storage medium of claim 11, wherein receiving the access token includes receiving an access token that is generated at the third party key storage server.

18. The method of claim 11, wherein sending the one or more messages over the network from the client to the third party key storage server and bypassing the authentication system includes sending an authentication credential from the client to the third party key storage server.

19. The method of claim 18 further including: receiving the authentication credential from the third party key storage server.

20. The method of claim 19, wherein sending the one or more messages over the network from the client to the third party key storage server and bypassing the authentication system includes sending the access token to the third party key storage server followed by sending the authentication credential, the key, and the request to encrypt the key from the client to the third party key storage server.

21. A system including processing circuitry; a memory operably coupled to the processing circuitry, that stores instructions which, when executed by the processing circuitry, cause the processing circuitry to perform operations comprising: sending a sign-up request, over a network by the client to an authentication service, for a user account associated with the decentralized application; receiving over the network at the client from the authentication service, an access token that corresponds to the sign-up request, for use at a third party key storage service; generating a key by the client; and sending over the network from the client to the third party key storage service and bypassing the authentication service, one or more messages that include the access token, the key, and a request to encrypt the key.