WHAT IS CLAIMED IS:

1. A method comprising:

generating, by a user device, a key recovery message comprising a public key or an identifier thereof associated with an account, the public key corresponding to a first private key associated with the user device;

providing, by the user device, the key recovery message to a smart contract on a blockchain;

receiving, by the user device, a recovery detected message from a server computer that monitors the smart contract; and

after providing the key recovery message to the smart contract, generating, by the user device, a new private key to replace the first private key.

2. The method of claim 1, further comprising:

providing, by the user device, collateral to the smart contract with the key recovery message.

3. The method of claim 1, wherein the new private key is generated by a cryptographic key process that allows the new private key to be used with the public key.

4. The method of claim 1, further comprising:

after receiving the recovery detected message, prompting, by the user device, a user to input a selection of dispute recovery, cancel recovery, or accept recovery.

5. The method of claim 1, wherein the server computer determines whether or not to cancel key recovery.

6. The method of claim 1, wherein the first private key is a first private key share and the second private key is a second private key share, wherein the first private key share and the second private key share are shares of a private key that corresponds to the public key.

7. The method of claim 6, wherein the new private key is a new private key share to replace the first private key share.

8. The method of claim 1, wherein after generating the new private key, the method further comprises:

generating, by the user device, a key update message comprising the new private key and a request to revoke the first private key;

generating, by the user device, a digital signature on the key update message using a third private key obtained prior to generating the key recovery message; and

providing, by the user device, the key update message comprising the digital signature to the smart contract.

9. The method of claim 8, wherein the smart contract verifies the digital signature using a group public key, revokes the first private key, and adds the new private key.

10. The method of claim 1, wherein after generating the new private key, the method further comprises:

generating, by the user device, a key update message comprising the new private key and a request to revoke the first private key;

generating, by the user device, a digital signature on the key update message using a third private key obtained prior to generating the key recovery message; and

providing, by the user device, the key update message comprising the digital signature to the server computer.

11. The method of claim 10, wherein the server computer verifies the digital signature using a group public key and signs the key update message with the second private key.

12. The method of claim 11, wherein the server computer provides the key update message with the digital signature that is further signed by the server computer using the second private key to the user device, wherein the method further comprises:

providing, by the user device, the key update message with the digital signature that is further signed by the server computer to the smart contract.

13. A user device comprising:

a processor; and

a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the processor for implementing themethod of any one of claims 1-12.

14. A method comprising:

detecting, by a server computer, a change to a smart contract on a blockchain, wherein the change is an inclusion of a key recovery message from a user device requesting recovery of a first private key;

determining, by the server computer, whether or not to cancel key recovery;

generating, by the server computer, a recovery detected message based on the determining; and

providing, by the server computer, the recovery detected message to the user device, wherein the user device generates a new private key to replace the first private key.

15. The method of claim 14, further comprising:

receiving, by the server computer, a key update message from the user device, wherein the key update message comprises the new private key and a digital signature formed by the user device using a third private key;

verifying, by the server computer, the digital signature using a group verification key; and

signing, by the server computer, the key update message using the second private key.

16. The method of claim 15, further comprising:

providing, by the server computer to the smart contract, the key update message that is signed by both the server computer using the second private key and by the user device using the third private key.

17. The method of claim 15, further comprising:

providing, by the server computer to the user device, the key update message that is signed by both the server computer using the second private key

and by the user device using the third private key, wherein the user device provides the key update message to the smart contract.

18. A server computer comprising:

a processor; and

a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the processor for implementing the method of any one of claims 14-17.