CLAIMS

What is claimed is:

1. A system comprising:

at least one processor;

at least one memory communicatively coupled to the at least one processor;

at least one network interface communicatively coupled to the at least one processor;

wherein the at least one processor is configured to:

receive a request to transfer a cryptographic token into a target transaction address from a remotely located computing device;

receive signed data from the remotely located computing device, the signed data signed by a private key;

receive at least one of the target transaction address or a target public key associated with the target transaction address from the remotely located computing device;

cryptographically verify that the at least one of the target transaction address or the target public key associated with the target transaction address is cryptographically derivable from the private key used to sign the signed data by inputting the private key and the signed data into a cryptographic verification algorithm that outputs a determination that the at least one of the target transaction address or the target public key associated with the target transaction address is cryptographically derivable from the private key used to sign the signed data;

verify, based on a whitelist, that the at least one of the target transaction address or the target public key associated with the target transaction address is whitelisted to receive transfer of the cryptographic token; and

transfer and record the transfer of the cryptographic token into the target transaction address on a blockchain only after: (1) cryptographically verifying that the at least one of the target transaction address or the target public key associated with the target transaction address is cryptographically derivable from the private key used to sign the signed data; and (2) verifying that the at least one of the target transaction address or the target public key

associated with the target transaction address is whitelisted to receive the transfer of the cryptographic token based on the whitelist.

2. The system of claim 1, wherein the at least one processor is configured to communicate data to the remotely located computing device to be signed by the remotely located computing device using the private key to create the signed data in response to the request to transfer the cryptographic token into the target transaction address being received from the remotely located computing device.

3. The system of any of claims 1-2, wherein the transfer of the cryptographic token into the target transaction address on the blockchain is recorded on an Ethereum blockchain.

4. A method for verifying a target transaction address is whitelisted to receive transfer of a cryptographic token before allowing transfer of the cryptographic token to the target transaction address, the method comprising:

receiving a request to transfer the cryptographic token into the target transaction address from a remotely located computing device;

receiving signed data from the remotely located computing device, the signed data signed by a private key;

receiving at least one of the target transaction address or a target public key associated with the target transaction address from the remotely located computing device;

cryptographically verifying that the at least one of the target transaction address or the target public key associated with the target transaction address is cryptographically derivable from the private key used to sign the signed data by inputting the private key and the signed data into a cryptographic verification algorithm that outputs a determination that the at least one of the target transaction address or the target public key associated with the target transaction address is cryptographically derivable from the private key used to sign the signed data;

verifying, based on a whitelist, that the at least one of the target transaction address or the target public key associated with the target transaction address is whitelisted to receive transfer of the cryptographic token; and

transferring and recording the transfer of the cryptographic token into the target transaction address on a blockchain only after: (1) cryptographically verifying that the at least one of the target transaction address or the target public key associated with the target transaction address is cryptographically derivable from the private key used to sign the signed data; and (2) verifying that the at least one of the target transaction address is whitelisted to receive the transfer of the cryptographic token based on the whitelist.

5. The method of claim 4, further comprising:

communicating data to the remotely located computing device to be signed by the remotely located computing device using the private key to create the signed data in response to the request to transfer the cryptographic token into the target transaction address being received from the remotely located computing device.

6. The method of any of claims 4-5, wherein recording the transfer of the cryptographic token into the target transaction address on the blockchain includes:

recording the transfer of the cryptographic token into the target transaction address on an Ethereum blockchain.

7. The system or method of any of claims 1-6, wherein the cryptographic token is configured to require at least one of the target transaction address or the target public key associated with the target transaction address to be whitelisted before allowing the transfer of the cryptographic token into the target transaction address.

8. The system or method of any of claims 1-7, wherein the signed data includes a signed string signed by the private key.

9. The system or method of any of claims 1-8, wherein the transfer of the cryptographic token only by whitelisted transaction addresses implements government regulations limiting who can purchase at least one of the cryptographic token and at least one asset represented by the cryptographic token.

10. The system or method of claim 9, wherein whitelisted transaction addressees are associated with individuals that comply with the government regulations limiting

who can purchase at least one of the cryptographic token and the at least one asset represented by the cryptographic token.

11. The system or method of any of claims 1-10, wherein the cryptographic token represents at least one of a security, a currency, a commodity, a bond, a fund, or a combination thereof.

12. The system or method of any of claims 1-11, wherein the cryptographic token is implemented using a smart contract.

13. The system or method of any of claims 1-12, wherein the whitelist is implemented using a smart contract, wherein the whitelist includes a list of target transaction addresses or target public keys associated with the target transaction addresses that are whitelisted to purchase the cryptographic token.

14. The system or method of any of claims 1-13, wherein the cryptographic token is implemented as an extension of Ethereum Request for Comment (ERC) 20.