

CLAIMS

What is claimed is:

1. A method comprising:
receiving, in a cryptoasset custodial system, a request to authorize a staking operation
5 for a proof-of-stake protocol associated with a blockchain, wherein the staking operation is associated with a private key of an asymmetric cryptographic key pair, the private key is usable to control ownership of a cryptoasset recorded in the blockchain, and the private key is securely held in the cryptoasset custodial system on behalf of a user of the cryptoasset custodial system;
10 performing, in response to the request, at least a portion of the proof-of-stake protocol in a hardware security module using logic designed for the proof-of-stake protocol, wherein the cryptoasset custodial system comprises the hardware security module, the hardware security module comprising at least one secure storage device and at least one physical computing device coupled with the at least one secure storage device, and the logic in the
15 hardware security module is configured to authorize the staking operation by digitally signing a staking transaction associated with the staking operation; and
sending the digitally signed staking transaction to another computer to effect the staking operation on behalf of the user.
2. The method of claim 1, wherein the cryptoasset custodial system comprises a relay
20 computer communicatively coupled with the hardware security module through an air gap that isolates the hardware security module from a network outside the cryptoasset custodial system, and the method comprises performing at least another portion of the proof-of-stake protocol in the relay computer.
3. The method of claim 2, comprising confirming, by the relay computer, that a format
25 of the staking transaction conforms to the proof-of-stake protocol, and performing the at least a portion of the proof-of-stake protocol in the hardware security module comprises reconfirming that the format of the staking transaction conforms to the proof-of-stake protocol.

4. The method of claim 2, wherein the cryptoasset custodial system comprises an online server computer communicatively coupled with the relay computer, the logic in the hardware security module comprises firmware code programmed to handle different staking transactions for two or more proof-of-stake protocols, and the method comprises:
- 5 performing an additional portion of the proof-of-stake protocol in the online server computer; and
- adjusting a timing control for the air gap based on the different staking transactions for the two or more proof-of-stake protocols.
5. The method of claim 1, comprising:
- 10 decrypting an encrypted key, in the hardware security module using a hardware-based cryptographic key securely stored in the hardware security module, to reveal a decrypted key;
- deriving, in the hardware security module, the private key of the asymmetric cryptographic key pair from at least the decrypted key;
- digitally signing, in the hardware security module, the staking transaction using the
- 15 private key derived in the hardware security module; and
- deleting the private key from memory in the hardware security module.
6. The method of claim 5, comprising:
- verifying, in the hardware security module, a policy map specifying individual users of the cryptoasset custodial system and a threshold number of the individual users to approve
- 20 the staking operation;
- validating, in the hardware security module, endorsement messages from at least a subset of the specified individual users of the cryptoasset custodial system by checking cryptographic digital signatures using public keys corresponding to the subset of the specified individual users; and
- 25 confirming, in the hardware security module, the staking operation is in accordance with control rules of the policy map when the endorsement messages have been validated for the threshold number of the specified individual users.
7. The method of claim 6, wherein the cryptoasset has been assigned to one of multiple different vaults in the cryptoasset custodial system, each of the multiple different vaults has a

vault-specific policy map that defines vault control rules governing which actions are allowed for the vault under one or more specified conditions, the policy map specifying the individual users is the vault-specific policy map corresponding to the one of the multiple different vaults to which the cryptoasset has been assigned, and deriving the private key
5 comprises regenerating the private key by applying a deterministic key derivation function to at least an identifier for the vault for the cryptoasset, an asset identifier for the cryptoasset, and the decrypted key.

8. A system comprising:
one or more hardware security modules, each of the one or more hardware security
10 modules comprising at least one secure storage device and at least one physical computing device coupled with the at least one secure storage device and configured to provide cryptographic processing to manage private keys of asymmetric cryptographic key pairs usable to control ownership of cryptoassets in at least one blockchain; and
one or more server computers communicatively coupled with the one or more
15 hardware security modules to access the cryptographic processing performed by the at least one physical computing device using the private keys;
wherein the at least one physical computing device of each of the one or more hardware security modules is configured to
check a requested staking action for a managed private key against a policy
20 map corresponding to the managed private key after authenticating the policy map based on a cryptographic key controlled by the hardware security module,
confirm that a format of the requested staking action conforms to a proof-of-stake protocol for the requested staking action,
digitally sign the requested staking action with the managed private key when
25 the requested staking action is authorized in accordance with the policy map and the format conforms to the proof-of-stake protocol, and
send the digitally signed staking action to another computer to effect one or more staking operations.

9. The system of claim 8, wherein the one or more server computers comprise at least
30 one relay server computer communicatively coupled with the hardware security module

through an air gap that isolates the hardware security, and the at least one relay server computer is configured to perform at least a portion of the proof-of-stake protocol.

10. The system of claim 9, wherein the one or more server computers comprise at least one online server computer communicatively coupled with the at least one relay server computer, the at least one online server computer being configured to accept requests from a public computer network and to perform an additional portion of the proof-of-stake protocol, each of the one or more hardware security modules comprises firmware configured to handle different staking transactions for two or more proof-of-stake protocols, and one or more of the at least one online server computer and the at least one relay server computer are configured to adjust a timing control for the air gap based on the different staking transactions for the two or more proof-of-stake protocols.

11. The system of claim 8, wherein the at least one physical computing device of each of the one or more hardware security modules is configured to
decrypt an encrypted key, using a hardware-based cryptographic key securely stored
in the hardware security module, to reveal a decrypted key;
derive the managed private key from at least the decrypted key;
digitally sign the requested staking action using the managed private key derived in the hardware security module; and
delete the managed private key from memory in the hardware security module.

12. The system of claim 11, wherein the at least one physical computing device of each of the one or more hardware security modules is configured to:
verify the policy map specifying individual users of the system and a threshold number of the individual users to approve a staking operation;
validate endorsement messages from at least a subset of the specified individual users by checking cryptographic digital signatures using public keys corresponding to the subset of the specified individual users; and
confirm the staking operation is in accordance with control rules of the policy map when the endorsement messages have been validated for the threshold number of the specified individual users.

13. The system of claim 12, wherein the private keys usable to control ownership of the cryptoassets are organized into logical groupings, each of the logical groupings has an associated policy map that defines rules governing which actions are allowed for the logical grouping under one or more specified conditions, the policy map specifying the individual
5 users is the policy map associated with one of the logical groupings corresponding to the managed private key, and the at least one physical computing device of each of the one or more hardware security modules is configured to derive the managed private key by applying a deterministic key derivation function to at least an identifier of the one of the logical groupings corresponding to the managed private key, an asset identifier, and the decrypted
10 key.

14. A computer-readable medium encoding a computer program operable to cause a hardware security module, comprising at least one secure storage device and at least one physical computing device coupled with the at least one secure storage device, to perform operations comprising:
15 receiving, in a cryptoasset custodial system, a request to authorize a staking operation for a proof-of-stake protocol associated with a blockchain, wherein the staking operation is associated with a private key of an asymmetric cryptographic key pair, the private key is usable to control ownership of a cryptoasset recorded in the blockchain, and the private key is securely held in the cryptoasset custodial system on behalf of a user of the cryptoasset
20 custodial system;
performing, in response to the request, at least a portion of the proof-of-stake protocol in a hardware security module using logic designed for the proof-of-stake protocol, wherein the logic in the hardware security module is configured to authorize the staking operation by digitally signing a staking transaction associated with the staking operation; and
25 sending the digitally signed staking transaction to another computer to effect the staking operation on behalf of the user.

15. The computer-readable medium of claim 14, wherein the cryptoasset custodial system comprises a relay computer communicatively coupled with the hardware security module through an air gap that isolates the hardware security module from a network outside the
30 cryptoasset custodial system.

16. The computer-readable medium of claim 15, wherein performing the at least a portion of the proof-of-stake protocol in the hardware security module comprises reconfirming that a format of the staking transaction conforms to the proof-of-stake protocol.

5 17. The computer-readable medium of claim 15, wherein the cryptoasset custodial system comprises an online server computer communicatively coupled with the relay computer, and the logic in the hardware security module comprises firmware code programmed to handle different staking transactions for two or more proof-of-stake protocols.

18. The computer-readable medium of claim 14, wherein the operations comprises:
decrypting an encrypted key, using a hardware-based cryptographic key securely
10 stored in the hardware security module, to reveal a decrypted key;
deriving the private key of the asymmetric cryptographic key pair from at least the decrypted key;
digitally signing the staking transaction using the private key derived in the hardware security module; and
15 deleting the private key from memory in the hardware security module.

19. The computer-readable medium of claim 18, wherein the operations comprises:
verifying a policy map specifying individual users of the cryptoasset custodial system and a threshold number of the individual users to approve the staking operation;
validating endorsement messages from at least a subset of the specified individual
20 users of the cryptoasset custodial system by checking cryptographic digital signatures using public keys corresponding to the subset of the specified individual users; and
confirming the staking operation is in accordance with control rules of the policy map when the endorsement messages have been validated for the threshold number of the specified individual users.

20. The computer-readable medium of claim 19, wherein the cryptoasset has been assigned to one of multiple different vaults in the cryptoasset custodial system, each of the multiple different vaults has a vault-specific policy map that defines vault control rules governing which actions are allowed for the vault under one or more specified conditions, the
- 5 policy map specifying the individual users is the vault-specific policy map corresponding to the one of the multiple different vaults to which the cryptoasset has been assigned, and deriving the private key comprises regenerating the private key by applying a deterministic key derivation function to at least an identifier for the vault for the cryptoasset, an asset identifier for the cryptoasset, and the decrypted key.