

CLAIMS

What is claimed is:

1. A method comprising:

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 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 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,

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 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;

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;

assigning the cryptoasset to one of multiple different vaults in the cryptoasset custodial system, each of the multiple different vaults having a vault-specific policy map that defines vault control rules governing which actions are allowed for the vault under one or more specified conditions;

generating, in the hardware security module, 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 a decrypted key controlled by the hardware security module;

digitally signing, in the hardware security module, using the logic in the hardware security module and the private key, a staking transaction associated with the staking operation when the staking operation is in accordance with control rules of the policy map and after the endorsement messages have been validated for the threshold number of the specified individual users including at least one required specific user; 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 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 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:

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:

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;

generating, 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

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 1, wherein verifying a policy map further comprises specifying individual users of the cryptoasset custodial system including at least one specific user whose approval is required.

7. The method of claim 1, wherein the cryptoasset custodial system further comprises a relay server connecting an online computer to the hardware security module, and wherein the method further comprises:

performing at least a portion of the proof-of-stake protocol by the relay server;
confirming, using the hardware security module, that a staking request is in a proper format for the proof-of-stake protocol; and
digitally signing, using the hardware security module, a staking transaction to authorize a staking operation after the hardware security module confirms that the staking request is in the proper format.

8. A non-transitory computer-readable medium, storing instructions executable by one or more computer processors of a cryptoasset custodial system, the instructions when executed by the one or more computer processors cause the one or more computer processors to perform operations comprising:

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 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, 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;

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 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;

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,

assigning the cryptoasset to one of multiple different vaults in the cryptoasset custodial system, each of the multiple different vaults having a vault-specific policy map that defines vault control rules governing which actions are allowed for the vault under one or more specified conditions;

generating, in the hardware security module, 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 a decrypted key controlled by the hardware security module;

digitally signing, in the hardware security module, using the logic in the hardware security module and the private key, a staking transaction associated with the staking operation when the staking operation is in accordance with control rules of the policy map and after the endorsement messages have been validated for the threshold number of the specified individual users; and

sending the digitally signed staking transaction to another computer to effect the staking operation on behalf of the user.

9. The non-transitory_computer-readable medium of claim 8, 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 cryptoasset custodial system.

10. The non-transitory_computer-readable medium of claim 9, 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.

11. The non-transitory_computer-readable medium of claim 9, 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.

12. The non-transitory_computer-readable medium of claim 8, wherein the operations comprise:

decrypting an encrypted key, using a hardware-based cryptographic key securely stored in the hardware security module, to reveal a decrypted key;

generating 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

deleting the private key from memory in the hardware security module.

13. The non-transitory_computer-readable medium of claim 8, wherein the cryptoasset custodial system, further comprises a relay server connecting an online computer to the hardware security module, wherein the cryptoasset has been assigned to one of multiple different vaults in the crypto asset custodial system, each of the multiple different vaults having a vault-specific policy map that defines vault control rules governing which actions are allowed for the vault under one or more specified conditions, wherein 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 wherein the operations further comprise:

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;

performing at least a portion of the proof-of-stake protocol by the relay server;

confirming, using the hardware security module, that a staking request is in a proper format for the proof-of-stake protocol; and

digitally signing using the hardware security module, a staking transaction to authorize a staking operation after the hardware security module confirms that the staking request is in the proper format.

14. The non-transitory computer-readable medium of claim 8, wherein verifying a policy map further comprises validating a policy map further specifying at least one specific user required for authorization of the transaction.

15. A cryptoasset custodial_system comprising:

one or more computer processors; and

a non-transitory computer-readable storage medium storing instructions executable by the one or more computer processors, the instructions when executed by the one or more computer processors causing the one or more computer processors to perform operations including:

receiving, in the 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 a hardware security module of the cryptoasset custodial system on behalf of a user of the cryptoasset custodial system;

performing, in response to the request, at least a portion of the proof-of-stake protocol in the 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;

verifying, 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 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;

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;

assigning the cryptoasset to one of multiple different vaults in the cryptoasset custodial system, each of the multiple different vaults having a vault-specific policy map that defines vault control rules governing which actions are allowed for the vault under one or more specified conditions;

generating, in the hardware security module, 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 a decrypted key controlled by the hardware security module;

digitally signing, in the hardware security module, using the logic in the hardware security module and the private key, a staking transaction associated with the staking operation, when the staking operation is in accordance with control rules of the policy map and after the endorsement messages have been validated for the threshold number of the specified individual users and wherein performing the at least a portion of the proof-of-stake protocol in the hardware security module comprises confirming that a format of the staking transaction conforms to the proof-of-stake protocol; and

sending the digitally signed staking transaction to another computer to effect the staking operation on behalf of the user.