

CLAIMS

What is claimed is:

1. A method comprising:

receiving, by a hardware security module, a request to take an action in a cryptoasset custodial system for an account holder registered with the cryptoasset custodial system, wherein the hardware security module comprises at least one secure storage device and at least one physical computing device coupled with the at least one secure storage device;

authenticating, by the hardware security module, a policy map associated with the action, wherein the policy map defines access control rules governing which actions are allowed under one or more specified conditions including a threshold number of endorsements needed to approve the action;

validating, by the hardware security module, at least two endorsement messages out of two or more received endorsement messages for the action by checking digital signatures of the two or more received endorsement messages, wherein

at least one of the validated endorsement messages has been generated by digital signing with a private key of a person, who is associated with the account holder, responsive to input from the person using a computing device that securely stores the private key of the person, and

at least one of the validated endorsement messages has been generated by digital signing with a private key of a program, which is associated with the account holder, responsive to the program confirming one or more circumstances specified by the account holder are met;

confirming, by the hardware security module, that the validated endorsement messages satisfy the threshold number of endorsements needed to approve the action in accordance with the authenticated policy map;

using, by the hardware security module, a private key associated with the action in a process of digitally signing data to authorize the action, wherein the private key has been decrypted, by the hardware security module, from an encrypted version of the private key using a hardware-based cryptographic key used by the hardware security module; and

sending, by the hardware security module, the digitally signed data to another computer to effect the action.

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.

3. The method of claim 2, wherein the action comprises a cryptoasset transaction for a specified cryptoasset.

4. The method of claim 3, wherein using a private key associated with the action in a process of digitally signing data to authorize the action comprises using a private key stored in the hardware security module to digitally sign data and to authorize withdrawal of a withdrawal amount of the specified cryptoasset and wherein the private key has been decrypted, by the hardware security module, from an encrypted version of the private key using a hardware-based cryptographic key stored on the hardware security module.

5. The method of claim 4, wherein the cryptoasset transaction comprises a specified destination for the withdrawal amount and wherein the method further comprises:

validating that the withdrawal amount is less than a threshold and authorizing the cryptoasset transaction only when the specified destination is a trusted destination.

6. The method of claim 5, wherein the program comprises custom logic and wherein the method further comprises:

receiving a request to add custom logic for an account holder;
determining if a quorum of authorized users for the account holder
approve addition of the custom logic; and
approving the custom logic at a risk analysis system of the cryptoasset
custodial system;
adding a custom logic key to an approval process for the account holder
when the quorum approves addition of the custom logic for the account holder and when the
risk analysis system approves the custom logic for the account holder.

7. The method of claim 1, wherein validating at least one of the validated endorsement messages has been generated by digital signing with a private key of a program responsive to the program confirming one or more circumstances specified by the account holder are met comprises confirming one or more circumstances specified by the account holder are met at a time when the program is run.

8. A method comprising:

receiving, by a hardware security module, a request to take an action in a cryptoasset custodial system for an account holder registered with the cryptoasset custodial system;

authenticating, by the hardware security module, a policy map associated with the action, wherein the policy map defines access control rules governing which actions are allowed under one or more specified conditions including a threshold number of endorsements needed to approve the action;

validating, by the hardware security module, at least two endorsement messages out of two or more received endorsement messages for the action by checking digital signatures of the two or more received endorsement messages, wherein

at least one of the validated endorsement messages has been generated by digital signing with a private key of a person, who is associated with the account holder, responsive to input from the person using a computing device that securely stores the private key of the person, and

at least one of the validated endorsement messages has been generated by digital signing with a private key of a program, which is associated with the account holder, responsive to the program confirming one or more circumstances specified by the account holder are met;

confirming, by the hardware security module, that the validated endorsement messages satisfy the threshold number of endorsements needed to approve the action in accordance with the authenticated policy map;

using, by the hardware security module, a private key associated with the action in a process of digitally signing data to authorize the action; and

sending, by the hardware security module, the digitally signed data to another computer to effect the action.

9. A system comprising:

one or more hardware security modules, each of the one or more hardware security 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 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:

receive a request to take an action in a cryptoasset custodial system for an account holder registered with the cryptoasset custodial system;

authenticate a policy map associated with the action, wherein the policy map defines access control rules governing which actions are allowed under one or more specified conditions including a threshold number of endorsements needed to approve the action;

validate at least two endorsement messages out of two or more received endorsement messages for the action by checking digital signatures of the two or more received endorsement messages, wherein

at least one of the validated endorsement messages has been generated by digital signing with a private key of a person, who is associated with the account holder, responsive to input from the person using a computing device that securely stores the private key of the person, and

at least one of the validated endorsement messages has been generated by digital signing with a private key of a program, which is associated with the account holder, responsive to the program confirming one or more circumstances specified by the account holder are met at a time when the program is run;

confirm that the validated endorsement messages satisfy the threshold number of endorsements needed to approve the action in accordance with the authenticated policy map;

use a private key associated with the action in a process of digitally signing data to authorize the action; and

send the digitally signed data to another computer to effect the action.

10. The system of claim 9, 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.

11. The system of claim 9, wherein the action comprises a cryptoasset transaction for a specified cryptoasset.

12. The system of claim 11, wherein using a private key associated with the action in a process of digitally signing data to authorize the action comprises using a private key stored in the hardware security module to digitally sign data and to authorize withdrawal of a withdrawal amount of the specified cryptoasset and wherein the private key has been decrypted, by the hardware security module, from an encrypted version of the private key using a hardware-based cryptographic key stored on the hardware security module.

13. The system of claim 12, wherein the cryptoasset transaction comprises a specified destination for the withdrawal amount and wherein the system further comprises:

validating that the withdrawal amount is less than a threshold and authorizing the crypto asset transaction only when the specified destination is a trusted destination.

14. The system of claim 12, wherein the program comprises custom logic and wherein the method further comprises:

receiving a request to add custom logic for an account holder;

determining if a quorum of authorized users for the account holder approve the addition of the custom logic; and

approving the custom logic at a risk analysis system of the cryptoasset custodial system;

adding a custom logic key to an approval process for the account holder when the quorum approves addition of the custom logic for the account holder and when the risk analysis system approves the custom logic for the account holder.

15. The system of claim 9, wherein validating at least one of the validated endorsement messages has been generated by digital signing with a private key of a program responsive to the program confirming one or more circumstances specified by the account holder are met comprises confirming one or more circumstances specified by the account holder are met at a time when the program is run.

16. 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:

receiving a request to take an action in a cryptoasset custodial system for an account holder registered with the cryptoasset custodial system;

authenticating a policy map associated with the action, wherein the policy map defines access control rules governing which actions are allowed under one or more specified conditions including a threshold number of endorsements needed to approve the action; validating at least two endorsement messages out of two or more received endorsement messages for the action by checking digital signatures of the two or more received endorsement messages, wherein

at least one of the validated endorsement messages has been generated by digital signing with a private key of a person, who is associated with the account holder, responsive to input from the person using a computing device that securely stores the private key of the person, and

at least one of the validated endorsement messages has been generated by digital signing with a private key of a program, which is associated with the account holder, responsive to the program confirming one or more circumstances specified by the account holder are met at a time when the program is run;

confirming that the validated endorsement messages satisfy the threshold number of endorsements needed to approve the action in accordance with the authenticated policy map;

using a private key associated with the action in a process of digitally signing data to authorize the action; and

sending the digitally signed data to another computer to effect the action.

17. The computer readable medium of claim 16, 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.

18. The computer readable medium of claim 17, wherein the action comprises a cryptoasset transaction for a specified cryptoasset.

19. The computer readable medium of claim 18, wherein using a private key associated with the action in a process of digitally signing data to authorize the action comprises using a private key stored in the hardware security module to digitally sign data and to authorize withdrawal of a withdrawal amount of the specified cryptoasset and wherein the private key has been decrypted, by the hardware security module, from an encrypted version of the private key using a hardware-based cryptographic key stored on the hardware security module.

20. The computer readable medium of claim 19, wherein the cryptoasset transaction comprises a specified destination for the withdrawal amount and wherein the method further comprises:

validating that the withdrawal amount is less than a threshold and authorizing the cryptoasset transaction only when the specified destination is a trusted destination.