

WHAT IS CLAIMED IS:

1. A method comprising:

transmitting, by a server computer of a cryptoasset custodial system, an approval request

for a cryptoasset transaction associated with a cryptoasset in accordance with a

policy stored in a hardware security module of the cryptoasset custodial system,

the hardware security module communicably coupled to the server computer, the

policy specifying at least one specific approver of the cryptoasset custodial

system required for approval of the cryptoasset transaction, the approval request

transmitted to a computer device associated with the at least one specific approver

and configured to cause the computer device to prompt the at least one specific

approver to approve the cryptoasset transaction;

receiving, by the server computer, a security key from a hardware security token

associated with the at least one specific approver, the security key indicating an

approval of the cryptoasset transaction;

authenticating, by a risk analysis module of the cryptoasset custodial system, an identity

of the at least one specific approver based on the security key, the risk analysis

module communicably coupled to the server computer;

responsive to the authenticating of the identity of the at least one specific approver:

signing, by the hardware security module, the cryptoasset transaction using a

cryptographic key stored in the hardware security module, the

cryptographic key being a private key of an asymmetric cryptographic key

pair associated with the cryptoasset transaction and usable to control

access to the cryptoasset; and

performing, by the server computer, the cryptoasset transaction on the cryptoasset using the cryptographic key.

2. The method of claim 1, wherein the hardware security token is one of a plurality of hardware security tokens, each hardware security token of the plurality of security tokens generating a different security key, and wherein each hardware security token is associated with a different approver of a plurality of approvers of the cryptoasset custodial system, the plurality of approvers comprising the at least one specific approver.
3. The method of claim 1, wherein the security key is a synchronous dynamic security key generated by the hardware security token and indexed by a timer of the hardware security token.
4. The method of claim 1, wherein the security key is an asynchronous one-time security key generated by the hardware security token using a cryptographic algorithm.
5. The method of claim 1, wherein the hardware security token comprises at least one of a smart card, a universal serial bus token, or a hardware dongle.
6. The method of claim 1, wherein the transmitting of the approval request comprises: generating, by the risk analysis module, a cryptographic authentication challenge based on a context of the cryptoasset transaction, the security key comprising a response

generated by the hardware security token to the cryptographic authentication challenge.

7. The method of claim 1, wherein the transmitting of the approval request is performed responsive to:
determining, by the hardware security module, that an endorsement of the cryptoasset transaction has been received from each user device of a plurality of user devices in satisfaction of a quorum for endorsing the cryptoasset transaction, each user device associated with a different user of the cryptoasset custodial system, the quorum specified by the policy.
8. A non-transitory computer-readable storage medium storing instructions executable by a cryptoasset custodial system, the instructions when executed by the cryptoasset custodial system cause the cryptoasset custodial system to:
transmit, by a server computer of the cryptoasset custodial system, an approval request for a cryptoasset transaction associated with a cryptoasset in accordance with a policy stored in a hardware security module of the cryptoasset custodial system, the hardware security module communicably coupled to the server computer, the policy specifying at least one specific approver of the cryptoasset custodial system required for approval of the cryptoasset transaction, the approval request transmitted to a computer device associated with the at least one specific approver and configured to cause the computer device to prompt the at least one specific approver to approve the cryptoasset transaction;

receive, by the server computer, a security key from a hardware security token associated with the at least one specific approver, the security key indicating an approval of the cryptoasset transaction;

authenticate, by a risk analysis module of the cryptoasset custodial system, an identity of the at least one specific approver based on the security key;

responsive to the authenticating of the identity of the at least one specific approver:

sign, by the hardware security module, the cryptoasset transaction using a cryptographic key stored in the hardware security module, the cryptographic key being a private key of an asymmetric cryptographic key pair associated with the cryptoasset transaction and usable to control access to the cryptoasset; and

perform, by the server computer, the cryptoasset transaction on the cryptoasset using the cryptographic key.

9. The non-transitory computer-readable storage medium of claim 8, wherein the hardware security token is one of a plurality of hardware security tokens, each hardware security token of the plurality of security tokens generating a different security key, and wherein each hardware security token is associated with a different approver of a plurality of approvers of the cryptoasset custodial system, the plurality of approvers comprising the at least one specific approver.
10. The non-transitory computer-readable storage medium of claim 8, wherein the security key is a synchronous dynamic security key generated by the hardware security token and indexed by a timer of the hardware security token.

11. The non-transitory computer-readable storage medium of claim 8, wherein the security key is an asynchronous one-time security key generated by the hardware security token using a cryptographic algorithm.
12. The non-transitory computer-readable storage medium of claim 8, wherein the hardware security token comprises at least one of a smart card, a universal serial bus token, or a hardware dongle.
13. The non-transitory computer-readable storage medium of claim 8, wherein the transmitting of the approval request comprises:
generating, by the risk analysis module, a cryptographic authentication challenge based on a context of the cryptoasset transaction, the security key comprising a response generated by the hardware security token to the cryptographic authentication challenge.
14. The non-transitory computer-readable storage medium of claim 8, wherein the transmitting of the approval request is performed responsive to:
determining, by the hardware security module, that an endorsement of the cryptoasset transaction has been received from each user device of a plurality of user devices in satisfaction of a quorum for endorsing the cryptoasset transaction, each user device associated with a different user of the cryptoasset custodial system, the quorum specified by the policy.
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 cause the one or more computer processors to:

transmit, by a server computer of the cryptoasset custodial system, an approval request for a cryptoasset transaction associated with a cryptoasset in accordance with a policy stored in a hardware security module of the cryptoasset custodial system, the hardware security module communicably coupled to the server computer, the policy specifying at least one specific approver of the cryptoasset custodial system required for approval of the cryptoasset transaction, the approval request transmitted to a computer device associated with the at least one specific approver and configured to cause the computer device to prompt the at least one specific approver to approve the cryptoasset transaction;

receive, by the server computer, a security key from a hardware security token associated with the at least one specific approver, the security key indicating an approval of the cryptoasset transaction;

authenticate, by a risk analysis module of the cryptoasset custodial system, an identity of the at least one specific approver based on the security key;

responsive to the authenticating of the identity of the at least one specific approver:

sign, by the hardware security module, the cryptoasset transaction using a cryptographic key stored in the hardware security module, the

cryptographic key being a private key of an asymmetric
cryptographic key pair associated with the cryptoasset transaction
and usable to control access to the cryptoasset; and
perform, by the server computer, the cryptoasset transaction on the cryptoasset
using the cryptographic key.

16. The cryptoasset custodial system of claim 15, wherein the hardware security token is one of a plurality of hardware security tokens, each hardware security token of the plurality of security tokens generating a different security key, and,
wherein each hardware security token is associated with a different approver of a plurality of approvers of the cryptoasset custodial system, the plurality of approvers comprising the at least one specific approver.
17. The cryptoasset custodial system of claim 15, wherein the security key is a synchronous dynamic security key generated by the hardware security token and indexed by a timer of the hardware security token.
18. The cryptoasset custodial system of claim 15, wherein the security key is an asynchronous one-time security key generated by the hardware security token using a cryptographic algorithm.
19. The cryptoasset custodial system of claim 15, wherein the hardware security token comprises at least one of a smart card, a universal serial bus token, or a hardware dongle.

20. The cryptoasset custodial system of claim 15, wherein the transmitting of the approval request comprises:
- generating, by the risk analysis module, a cryptographic authentication challenge based on a context of the cryptoasset transaction, the security key comprising a response generated by the hardware security token to the cryptographic authentication challenge.