CLAIMS

What is claimed is:

1. A method of authorizing an action, the method comprising:

receiving, at ~~a~~ an online server ~~system~~, an action request for a requested action involving a digital asset;

~~using~~ determining, by a hardware security module in communication with the online server, ~~system to determine~~ whether a policy-based quorum of a plurality of users has approved the requested action, by using a public key of a public-private key pair for each of the plurality of users; and

only after determining that the policy-based quorum of the plurality of users has approved of the requested action, approving, ~~the action~~ by ~~using~~ the hardware security module, the action by signing ~~to sign~~ an approval message for the action with a cryptographic key associated with the digital asset, wherein the cryptographic key associated with the digital asset ~~that is~~ stored only in the hardware security module, wherein the cryptographic key associated with the digital asset is generated by the hardware security module for a blockchain address associated with the digital asset, and wherein the hardware security module does not permit the cryptographic key to be read by any entity outside the hardware security module.

2. A method as recited in claim 1, wherein, for each of the plurality of users, a private key of the public-private key pair for said user is stored within a secure storage of a mobile device associated with said user.

3. A method as recited in claim 1, wherein the requested action comprises a requested transaction involving a digital asset.

4. A method as recited in claim ~~1~~3, further comprising sending the transaction onto a blockchain network in response to approving the transaction.

5. A method as recited in claim 1, wherein the requested action comprises a requested transaction involving ~~an~~ the digital asset, wherein the cryptographic key is a private key of a public-private key pair associated with the digital asset, the method further comprising using the hardware security module to generate the cryptographic key.

6. A method as recited in claim 1, further comprising:

causing an endorsement request message to be transmitted to each of a plurality of user devices, each of the plurality of user devices associated with a

different one of the plurality of users, each endorsement request message being configured to cause a receiving user device to prompt a corresponding user to endorse the requested transaction.

7. A method as recited in claim 6, further comprising:

for at least two of the user devices, verifying, at the online server ~~system~~, that the user device has authenticated a corresponding user by use of a biometric authentication technique, in connection with an endorsement of the requested transaction.

8. A method of authorizing a transaction involving a cryptoasset, the method comprising:

receiving, at ~~a~~ an online server ~~system~~, a transaction request for a requested transaction involving the cryptoasset;

receiving, at the online server ~~system~~, at least one endorsement message from at least one user device, each said at least one endorsement message being associated with a different one of a plurality of users;

determining, by a hardware security module in communication with the online server ~~system~~, whether the at least one endorsement message satisfies a quorum for approving the requested transaction, the quorum being defined in a stored policy associated with the cryptoasset; and

only if the at least one endorsement message satisfies the quorum, then authorizing, by the hardware security module, the requested transaction by using ~~the hardware security module to sign an approval of the requested transaction with~~ a private key associated with the cryptoasset to sign an approval of the requested transaction, wherein the private key is generated by the hardware security module for a blockchain address associated with the cryptoasset, and wherein the private key only exists within the hardware security module and is inaccessible by devices external to the hardware security module.

9. A method as recited in claim 8, further comprising:

for at least one user device of said at least one user device, verifying, at the online server ~~system~~, that the user device has authenticated a corresponding user by a first biometric authentication technique, in connection with an endorsement of the requested transaction.

10. A method as recited in claim 9, further comprising using a second biometric authentication technique at the online server ~~system~~ to authenticate at least one of the users in connection with an endorsement of the requested action.

11. A method as recited in claim 8, further comprising using an authentication technique at the online server ~~system~~ to authenticate a user in connection with an endorsement of the requested transaction, the authentication technique including:

causing a user device of the user to output a prompt the user to record and upload to the online server ~~system~~ a video in which the user performs a specified action or speaks specified content;

receiving at the online server ~~system~~ a video uploaded responsive to the prompt; and

analyzing the video at the online server ~~system~~ to authenticate the user by performing at least one of:

verifying a biometric characteristic of the user from the video, or

verifying that the user performed the specified action or spoke the specified content in the video.

12. A method as recited in claim 8, further comprising:

causing a user device of at least one of the users to output a deterministic authentication challenge to the corresponding user, wherein a content of the deterministic authentication challenge is based on a context of the requested transaction.

13. A method as recited in claim 8, further comprising:

in response to the transaction request, invoking a risk analysis of the requested transaction;

wherein said authorizing the transaction is done only if a result of the risk analysis indicates that a risk level associated with the requested transaction satisfies a risk criterion and the at least one endorsement message satisfies the quorum.

~~14. A method as recited in claim 8, further comprising:~~

~~using the hardware security module to generate the private key associated with the cryptoasset.~~

~~15~~14. A method as recited in claim 8, ~~further comprising:~~

~~using~~ wherein the private key associated with the cryptoasset is generated by the hardware security module ~~to generate the private key associated with the cryptoasset~~ as part of a public-private key pair associated with the cryptoasset.

~~16. A method as recited in claim 15, further comprising:~~

~~storing the private key associated with the cryptoasset within the hardware security module, wherein the private key associated with the cryptoasset cannot be read by or transmitted to any entity that is external to the hardware security module.~~

~~17~~15. A method as recited in claim 8, further comprising:

storing in the hardware security module a public key of a public-private key pair for each said at least one user device.

~~18~~16. A method as recited in claim ~~17~~15, wherein each endorsement message has been signed by a corresponding user device with the private key of the public-private key pair associated with said corresponding user device.

~~19~~17. A method as recited in claim ~~17~~15, further comprising:

providing a data package to the hardware security module prior to said authorizing the requested transaction, the data package including data indicative of the quorum and a public key associated with each said at least one user device.

~~20~~18. A method as recited in claim 8, wherein the hardware security module has no direct connection to any public computer network.

~~21~~19. A method as recited in claim 8, ~~storing, in a hardware security module, a private key associated with the cryptoasset,~~ wherein the private key ~~being~~ of the cryptoasset is part of a public-private key pair associated with the cryptoasset.

~~22~~20. A method as recited in claim 8, causing, by the online server ~~computer system~~, an endorsement request message to be transmitted to each said at least one user device, each endorsement request message being configured to cause the receiving user device to prompt a corresponding user to endorse the requested transaction.

~~23~~21. A method as recited in claim 8, storing the policy associated with the cryptoasset, the policy defining a quorum of a plurality of users required for authorization of the transaction.

~~24~~22. A method as recited in claim 8, wherein the determining whether the at least one endorsement message satisfies a quorum defined in a policy associated with the cryptoasset is ~~done~~ performed by using a public key associated with the user device that sent each endorsement message to validate the corresponding endorsement message.

~~25~~23. A method as recited in claim 8, wherein the at least one endorsement message has been generated by signing on the user device using a private key stored in a secure storage of the user device.

~~26~~24. A method as recited in claim 8, further comprising:

~~sending~~ transmitting to the hardware security module a data package that includes data specifying the policy, including the quorum, and a public key associated with each said at least one user device.

~~27~~25. A method of authorizing a transaction, the method comprising:

receiving, at ~~a~~ an online server ~~computer system~~ from a user device via a public computer network, a transaction request for a requested transaction relating to a cryptoasset;

in response to the transaction request, invoking a risk analysis of the requested transaction;

accessing, by the online server ~~computer system~~, a stored policy associated with the cryptoasset, the policy specifying a quorum of a plurality of users required for authorization of the transaction;

causing, by the online server ~~computer system~~, an endorsement request message to be transmitted to each of a plurality of mobile devices, each of the mobile devices being associated with a different one of the plurality of users, each endorsement request message being configured to cause the receiving mobile device to prompt a corresponding user to endorse the requested transaction;

receiving, at the online server ~~computer system~~, an endorsement message from at least one of the mobile devices, each endorsement message indicative of an endorsement of the requested transaction by a user using a corresponding one of the mobile devices, each endorsement message having been signed by the corresponding mobile device with a private key stored in a secure storage in the corresponding mobile device;

storing, in a hardware security module that has no direct connection to any public computer network, a private key associated with the cryptoasset, the private key being part of a public-private key pair associated with the cryptoasset, the hardware security module in communication with the online server;

determining, by the hardware security module, whether a valid endorsement has been received from each of two or more of the mobile devices in satisfaction of the quorum specified in the policy, by using a public key associated with the mobile device that sent each endorsement message to validate the corresponding endorsement message; and

only if the risk analysis has determined that a level of risk associated with the requested transaction is below a threshold and a valid endorsement of the requested transaction has been received from each of two or more of the mobile devices in satisfaction of the quorum, then authorizing, by the hardware security module, the transaction by using the ~~hardware security module~~ private key associated with the cryptoasset to sign an approval of the requested transaction ~~with the private key associated with the cryptoasset~~, wherein the private key is generated by the hardware security module for a blockchain address associated with the cryptoasset, and wherein the private key only exists within the hardware security module and is inaccessible by devices external to the hardware security module.

~~28~~26. A digital asset custodial system comprising:

an online server ~~subsystem~~ configured to receive a requested transaction relating to a digital asset from a user via a public computer network and to cause an endorsement request to be sent to at least one mobile device according to a stored

policy in response to receipt of the requested transaction, ~~each said~~ the at least one mobile device being associated with at least one of a plurality of users specified in the policy as possible members of a quorum for approving the transaction, the online

server ~~subsystem~~ further configured to receive an endorsement message from the corresponding mobile device of one or more of the plurality of users; and

a hardware security module in communication with the online server, the hardware security module configured to receive an indication of the endorsement message from a mobile device of one or more of the users, to determine whether valid endorsements have been received from each of two or more of the users in satisfaction of the quorum specified in the policy, based on a public key associated with each of the plurality of users for which an endorsement message has been received, and to authorize the transaction by signing an approval of the requested transaction with a private key associated with the digital asset only if a valid endorsement of the requested transaction has been received from each of two or more of the users in satisfaction of the quorum, wherein the private key is generated by the hardware security module for a blockchain address associated with the digital asset, and wherein the private key only exists within the hardware security module and is inaccessible by devices external to the hardware security module.

~~29~~27. A digital asset custodial system as recited in claim ~~28~~26, further comprising a relay server to isolate the security module from the Internet.

~~30~~28. A digital asset custodial system as recited in claim ~~28~~26, further comprising a risk analysis module to assign a risk score to the requested transaction.

~~31~~29. A digital asset custodial system as recited in claim ~~28~~26, the online server ~~subsystem~~ further being configured to cause an endorsement request message to be transmitted to each of a plurality of mobile devices, each endorsement request message being configured to cause the receiving mobile device to prompt a corresponding user to endorse the requested transaction.

~~32~~30. A digital asset custodial system as recited in claim ~~28~~26, wherein the hardware security module is further configured to:

generate the private key associated with the digital asset as part of a public-private key pair associated with the digital asset;

provide a public key of the public-private key pair associated with the digital asset to a computer system that is external to the hardware security module; and

maintain the private key of the public-private key pair associated with the digital asset in a storage within the hardware security module ~~and prevent the private~~

~~key of the public-private key pair associated with the digital asset cannot from being read by any entity that is external to the hardware security module~~.

~~33~~31. A digital asset custodial system as recited in claim ~~28~~26, and configured to verify, for at least one user device, that the user device has authenticated a corresponding user by a first biometric authentication technique, in connection with an endorsement of the requested transaction.

~~34~~32. A digital asset custodial system as recited in claim ~~33~~31, further configured to use a second biometric authentication technique to authenticate at least one of the users in connection with endorsement of the requested action.

~~35~~33. A digital asset custodial system as recited in claim ~~28~~26, and configured to authenticate a user in connection with endorsement of the requested transaction, by:

causing a user device of the user to output a prompt to the user to record and upload to the server system a video in which the user performs a specified action or speaks specified content;

receiving a video uploaded responsive to the prompt; and

analyzing the video to authenticate the user by performing at least one of

verifying a biometric characteristic of the user from the video, or

verifying that the user performed the specified action or spoke the specified content in the video.

~~36~~34. A digital asset custodial system as recited in claim ~~28~~26, and configured to cause a user device of at least one of the users to output a deterministic authentication challenge to the corresponding user, wherein a content of the deterministic authentication challenge is based on a context of the requested transaction.

~~37. A hardware security module comprising:~~

~~a non-volatile storage to store cryptographic data;~~

~~a communication interface through which to communicate with a host computer system; and~~

logic circuitry coupled to the non-volatile storage and the communication interface and configured to cause the hardware security module to perform operations including:

receiving an indication of a deposit of a digital asset, from a calling process;

in response to the indication,

generating a public-private key pair associated with the digital asset,

providing a public key of the public-private key pair to the calling process, and

storing the private key of the public-private key pair in the non-volatile storage in a protected manner;

receiving an indication of a requested operation related to the digital asset, an indication of a quorum of users whose endorsements of the requested operation are required to authorize the requested transaction, and a public key associated with each of one or more of the plurality of users who ostensibly have endorsed the requested transaction;

determining whether a valid endorsement has been received from two or more users of the plurality of users in satisfaction of the quorum, based on the indication of the quorum and the public key associated with each of one or more users who ostensibly endorsed the requested transaction; and

after a determination that a valid endorsement has been received from two or more users in satisfaction of the quorum, authorizing the requested transaction by signing an approval of the requested transaction with the private key of the public-private key pair associated with the digital asset.

38. A hardware security module as recited in claim 37, wherein the private key of the public-private key pair associated with the digital asset is prevented from being read by any entity external to the hardware security module.

39. A hardware security module as recited in claim 37, the operations further including causing the transaction to be transmitted onto a blockchain network only after said signing the approval of the transaction.

~~40. A method comprising:~~

~~receiving, at first user device associated with a user, a first message including a transaction description relating to a requested transaction, from a server system via a public computer network;~~

~~in response to the first message, transmitting a second message including an indication of the transaction from the first user device to a second user device associated with the user, via a first point-to-point channel that is isolated from the public computer network, wherein the second user device is isolated from the public computer network, the second message to cause the second user device to output a description of the transaction and to prompt the user to endorse the transaction;~~

~~receiving, at the first user device from the second user device, a third message indicative that the user has used the second user device to endorse the transaction, the third message being received via the first point-to-point channel or via a second point-to-point channel that is isolated from the public computer network; and~~

~~in response to the third message, sending a fourth message indicative that the user has endorsed the transaction, from the first user device to the server system via the public computer network.~~