

WHAT IS CLAIMED IS:

1. A cryptoasset custodial system comprising:
a server computer configured to:
transmit an endorsement request for a cryptoasset transaction to be performed by
the server computer on a blockchain, the endorsement request transmitted
to a user device associated with a user of the cryptoasset custodial system
and configured to cause the user device to prompt the mobile user to
endorse the cryptoasset transaction;
receive a plurality of data points collected from one or more mobile devices
communicably coupled to the user device and associated with the user, the
plurality of data points indicating an identity of the user; and
receive a cryptographic endorsement of the cryptoasset transaction from the user
device; and
a risk analysis module communicably coupled to the server computer and configured to:
generate, on a risk review dashboard, a graphical visualization comprising a risk
metric based on the plurality of data points, the risk metric indicating a
risk of accepting the cryptographic endorsement of the cryptoasset
transaction from the user device, the generating of the graphical
visualization comprising:
determining whether the plurality of data points matches expected values.
2. The cryptoasset custodial system of claim 1, further comprising:

a hardware security module communicably coupled to the server computer via a relay server and configured to:

receive the cryptographic endorsement of the cryptoasset transaction from the server computer via the relay server, responsive to the risk metric being below a threshold risk metric; and

generate a cryptographic key associated with the cryptoasset transaction and usable to control access to the blockchain.

3. The cryptoasset custodial system of claim 1, wherein the risk analysis module is further configured to:

register each mobile device of the one or more mobile devices on the cryptoasset custodial system prior to the receiving of the plurality of data points, the registering of each mobile device performed responsive to receiving, by the server computer, a registration request from the user device, the registration request associating the user of the cryptoasset custodial system with each mobile device.

4. The cryptoasset custodial system of claim 3, wherein the registering of each mobile device comprises assigning, to each mobile device, a required status or a non-required status, the risk analysis module further configured to:

detect absence of a data point collected from a mobile device of the one or more mobile devices based on the plurality of data points, wherein the mobile device is assigned the required status; and

increase the risk metric responsive to the detecting of the absence.

5. The cryptoasset custodial system of claim 1, wherein the graphical visualization further comprises a trend of the plurality of data points, and wherein the risk analysis module is further configured to determine the expected value of the plurality of data points based on the trend.
6. A method comprising:
transmitting, by a server computer, an endorsement request for a cryptoasset transaction to a user device associated with a user and configured to cause the user device to prompt the user to endorse the cryptoasset transaction;
receiving, by the server computer, a plurality of data points collected from one or more mobile devices associated with the user, the plurality of data points indicating an identity of the user;
receiving, by the server computer, a cryptographic endorsement of the cryptoasset transaction from the user device; and
generating, by a risk analysis module, a graphical visualization comprising a risk metric based on the plurality of data points, the risk metric indicating a risk of accepting the cryptographic endorsement from the user device, the generating of the graphical visualization comprising:
determining whether the plurality of data points matches expected values.
7. The method of claim 6, further comprising:
responsive to the risk metric being below a threshold risk metric, transmitting, from the server computer, the cryptographic endorsement through a relay server to a hardware security module; and

generating, by the hardware security module, a cryptographic key associated with the cryptoasset transaction.

8. The method of claim 6 further comprising:
registering, by the risk analysis module, each mobile device of the one or more mobile devices prior to the receiving of the plurality of data points, the registering of each mobile device performed responsive to receiving, by the server computer, a registration request from the user device, the registration request associating the user with each mobile device.
9. The method of claim 8, wherein the registering of each mobile device comprises assigning, to each mobile device, a required status or a non-required status, the method further comprising:
detecting, by the risk analysis module, absence of a data point collected from a mobile device of the one or more mobile devices based on the plurality of data points, wherein the mobile device is assigned the required status; and
increasing, by the risk analysis module, the risk metric responsive to the detecting of the absence.
10. The method of claim 6, wherein a mobile device of the one or more mobile devices is a smartwatch or a fitness tracker of the user, and
wherein the plurality of data points comprises a geographical location of the smartwatch or the fitness tracker measured by a global positioning system receiver of the smartwatch or the fitness tracker.

11. The method of claim 6, wherein the plurality of data points comprises at least one of:
an identification number of a mobile device of the one or more mobile devices;
an altitude of the mobile device relative to sea level measured by the mobile device;
a service set identifier of a wireless network that the mobile device is connected to; or
a Bluetooth device address of the mobile device.
12. The method of claim 6, further comprising:
detecting, by the risk analysis module, a mismatch between a first data point of the plurality of data points and a second data point of the plurality of data points, the first data point collected from a first mobile device of the one or more mobile devices and the second data point collected from a second mobile device of the one or more mobile devices; and
increasing, by the risk analysis module, the risk metric responsive to the detecting of the mismatch.
13. The method of claim 6, wherein the generating of the graphical visualization further comprises:
extracting, by a feature extraction module, a feature vector based on the plurality of data points; and
generating, by a machine learning module, the risk metric based on the feature vector, the machine learning module trained to indicate the risk of accepting the cryptographic endorsement based on whether the plurality of data points matches the expected values.

14. 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 endorsement request for a cryptoasset transaction to a user device associated with a user of the cryptoasset custodial system and configured to cause the user device to prompt the user to endorse the cryptoasset transaction;
 - receive, by the server computer, a plurality of data points collected from one or more mobile devices associated with the user and indicating an identity of the user;
 - receive, by the server computer, a cryptographic endorsement of the cryptoasset transaction from the user device; and
 - generate, by a risk analysis module of the cryptoasset custodial system, a graphical visualization comprising a risk metric based on the plurality of data points, the risk metric indicating a risk of accepting the cryptographic endorsement from the user device, the generating of the graphical visualization comprising:
 - determining whether the plurality of data points matches expected values.
15. The non-transitory computer-readable storage medium of claim 14, wherein the instructions further cause the cryptoasset custodial system to:
- responsive to the risk metric being below a threshold risk metric, transmit, from the server computer, the cryptographic endorsement through a relay server to a hardware security module of the cryptoasset custodial system; and
 - generate, by the hardware security module, a cryptographic key associated with the cryptoasset transaction.

16. The non-transitory computer-readable storage medium of claim 14, wherein the instructions further cause the cryptoasset custodial system to:
- register, by the risk analysis module, each mobile device of the one or more mobile devices prior to the receiving of the plurality of data points, the registering of each mobile device performed responsive to receiving, by the server computer, a registration request from the user device, the registration request associating the user with each mobile device.
17. The non-transitory computer-readable storage medium of claim 16, wherein the registering of each mobile device comprises assigning, to each mobile device, a required status or a non-required status, the instructions further causing the cryptoasset custodial system to:
- detect, by the risk analysis module, absence of a data point collected from a mobile device of the one or more mobile devices based on the plurality of data points, wherein the mobile device is assigned the required status; and
- increase, by the risk analysis module, the risk metric responsive to the detecting of the absence.
18. The non-transitory computer-readable storage medium of claim 14, wherein a mobile device of the one or more mobile devices is a smartwatch or a fitness tracker of the user, and
- wherein the plurality of data points comprises a geographical location of the smartwatch or the fitness tracker measured by a global positioning system receiver of the smartwatch or the fitness tracker.

19. The non-transitory computer-readable storage medium of claim 14, wherein the plurality of data points comprises at least one of:
- an identification number of a mobile device of the one or more mobile devices;
 - an altitude of the mobile device relative to sea level measured by the mobile device;
 - a service set identifier of a wireless network that the mobile device is connected to; or
 - a Bluetooth device address of the mobile device.
20. The non-transitory computer-readable storage medium of claim 14, wherein the instructions further cause the cryptoasset custodial system to:
- detect, by the risk analysis module, a mismatch between a first data point of the plurality of data points and a second data point of the plurality of data points, the first data point collected from a first mobile device of the one or more mobile devices and the second data point collected from a second mobile device of the one or more mobile devices; and
 - increase, by the risk analysis module, the risk metric responsive to the detecting of the mismatch.