multi-signature payment account, wherein the payment account is encrypted according to a first key generated by a client computer, a second key generated by the exchange server, and a third key generated by an oracle server, and wherein the payment account is accessible when decrypted by at least two keys of the first key, the second key, and the third key; monitor a first public blockchain asset record, a transfer of a first digital asset from the client computer to the encrypted multi-signature payment account; monitor a second public blockchain asset record, a transfer of a second digital asset from a second client computer, to an account having a payment address associated with the client computer; and upon verifying, via the second public blockchain asset record, a transfer of the second digital asset to an account associated with the client computer: sign the first blockchain of the first digital asset, wherein the oracle server signs the first blockchain using the third key.

[0012a] According to an aspect, there is provided a computer-implemented method of swapping possession of blockchain assets according to a zero-custody switch, the method comprising: generating, by the exchange server, a multi-signature payment account on a blockchain of the first digital asset, wherein funds in the multi-signature payment account are transferable with signatures of at least two of: a customer private cryptographic key generated by the customer, an exchange private cryptographic key generated by the exchange server, and an oracle private cryptographic key generated by an oracle server; monitoring, by the exchange server, the multi-signature payment account for a payment of the first digital asset according to a non-custodial order specified by a customer to swap a first digital asset for a second digital asset; monitoring, by the exchange server, a final address on a blockchain of the second digital asset for a payment of the second digital asset according to the non-custodial order to determine whether the non-custodial order is a completed order; and upon verifying the non-custodial order is a completed order, by the exchange server, accessing funds in the multi-signature payment account by signing with the exchange private cryptographic key a blockchain transaction moving funds out of the multi-signature payment account to a merchant account controlled by the exchange server, wherein the oracle server co-signs the blockchain transaction with the oracle private key according to application of a set of oracle non-custodial switch rules.

[0013] It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory and are intended to provide further explanation of the invention as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The accompanying drawings constitute a part of this specification and illustrate an embodiment of the invention and together with the specification, explain the invention.

[0015] **FIG. 1** shows components of an embodiment in accordance with the present disclosure.

[0016] **FIG. 2** depicts the components of an embodiment of a network in accordance with the present disclosure.

[0017] **FIG. 3** depicts a flow chart illustrating the steps in an embodiment of the present disclosure.

[0018] **FIG. 4** depicts a flow chart illustrating the steps in an embodiment of the present disclosure.

[0019] **FIG. 5** depicts a flow chart illustrating the steps in an embodiment of the present disclosure.

CLAIMS

1. A computer-implemented method of swapping possession of blockchain assets according to a zero-custody switch, the method comprising:

generating, by the exchange server, a multi-signature payment account on a blockchain of the first digital asset, wherein funds in the multi-signature payment account are transferable with signatures of at least two of: a customer private cryptographic key generated by the customer, an exchange private cryptographic key generated by the exchange server, and an oracle private cryptographic key generated by an oracle server;

monitoring, by the exchange server, the multi-signature payment account for a payment of the first digital asset according to a non-custodial order specified by a customer to swap a first digital asset for a second digital asset;

monitoring, by the exchange server, a final address on a blockchain of the second digital asset for a payment of the second digital asset according to the non-custodial order to determine whether the non-custodial order is a completed order; and

upon verifying the non-custodial order is a completed order, by the exchange server, accessing funds in the multi-signature payment account by signing with the exchange private cryptographic key a blockchain transaction moving funds out of the multi-signature payment account to a merchant account controlled by the exchange server, wherein the oracle server co-signs the blockchain transaction with the oracle private key according to application of a set of oracle non-custodial switch rules.

2. The method according to claim 1, further comprising:

transmitting, by the exchange server, to a payment address associated with the customer an update indicating custody for the first digital asset to the customer.

3. The method according to claim 1, wherein generating the multi-signature payment account further comprises receiving, by the exchange server, from the customer a first seed value.

4. The method according to claim 1, wherein the oracle server is a decentralized autonomous organization (DAO).

5. The method according to claim 1, further comprising generating, by the exchange server, a second seed based upon a portion of the exchange private cryptographic key generated by the exchange server.

6. The method according to claim 1, wherein the operation that signs with the exchange private cryptographic key the blockchain transaction verifies the non-custodial order is a partially filled order and the blockchain transaction moves a proportionate amount of the funds out of the multi-signature payment account to a merchant account controlled by the exchange server.

7. The method according to claim 1, wherein the oracle switch rules are based at least in part on fulfillment of the non-custodial order.

8. The method according to claim 6, further comprising:

generating a refund blockchain transaction, the refund blockchain transaction moving a proportionate amount of the funds out of the multi-signature payment account to a refund address controlled by the customer.

9. The method according to claim 1, wherein verifying the transfer of the second digital asset further comprises:

receiving, by the exchange server, an update to the second blockchain indicating custody of the second digital asset from a second client to a first client.

10. The method according to claim 1, wherein the non-custodial order is not a completed order by an expiration of a time threshold and wherein the oracle server co-signs the blockchain transaction with the oracle private cryptographic key and the customer co-signs the blockchain transaction with the customer private cryptographic key, the blockchain transaction moving funds out of the multi-signature payment account to a refund address controlled by the customer.

11. A computing system for exchanging blockchain-based digital assets, the system comprising:

an exchange server hosted on one or more server computers comprising a processor, the exchange server configured to carry out the method of any preceding claim.