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 method of ordering an exchange of digital assets via a zero-custody switch, the method comprising: generating a limit order request for a non-custodial exchange of a first digital asset for a second digital asset, the first digital asset being held by a customer, and the second digital asset being held by a counterparty; generating a cryptographic key pair including a customer private key and a customer public key; transmitting, to an oracle, a refund address, a final payment address, and the customer public key; receiving a payment address having an encumbrance; and broadcasting a deposit transaction to a network of the first digital asset, the deposit transaction transferring a purchase amount of the first digital asset to the payment address.

[0012b] According to another aspect, there is provided a method for securing the exchange of digital assets via a zero-custody switch: receiving an order request for a non-custodial exchange of a first digital asset for a second digital asset, the first digital asset being held by a customer and the second digital asset being held by a counterparty, the request including a final payment address of the customer; generating a cryptographic key pair including a counterparty public key and a counterparty private key; receiving a payment address, the payment address having an encumbrance depending at least on a digital signature of at least two of the counterparty private key, a customer private key, and an oracle private key; determining whether the payment address satisfies a funding condition; and broadcasting one or more completion transactions based at least in part on whether the payment address satisfies the funding condition.

[0012c] According to yet another aspect, there is provided a non-transitory computer-readable medium encoded with instructions for operating a zero-custody switch, the instructions comprising: receiving an order request to exchange a first digital asset for a second digital asset, the order request including a final payment address of a customer and a refund address of the customer; receiving a customer public key and a counterparty public key; generating a key pair including a

private oracle key and a public oracle key; receiving a payment address for funding the order request, the payment address having an encumbrance; determining whether the payment address satisfies a funding condition; determining whether the final payment address of the customer satisfies a final payment condition; and signing a completion transaction with the private oracle key, the completion transaction being a release transaction spending funds in the payment address to a counterparty address if the funding condition and the final payment condition are satisfied, and the completion transaction being a refund transaction spending funds in the payment address to the refund address of the customer if the final payment condition is not satisfied.

[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 method of ordering an exchange of digital assets via a zero-custody switch, the method comprising:

generating a limit order request for a non-custodial exchange of a first digital asset for a second digital asset, the first digital asset being held by a customer, and the second digital asset being held by a counterparty;

generating a cryptographic key pair including a customer private key and a customer public key;

transmitting, to an oracle, a refund address, a final payment address, and the customer public key;

receiving a payment address having an encumbrance; and

broadcasting a deposit transaction to a network of the first digital asset, the deposit transaction transferring a purchase amount of the first digital asset to the payment address.

2. The method of claim 1, further comprising:

pre-signing a refund transaction with the customer private key; and

transmitting the refund transaction to the oracle.

3. The method of claim 1, wherein the encumbrance is satisfied by digital signatures of at least two of the customer private key, a counterparty private key, and an oracle private key.

4. The method of claim 1, wherein the limit order request includes an expiration time and at least one unlocking script satisfying the encumbrance depends at least in part on the expiration time.

5. The method of claim 1, wherein the first digital asset is tracked on a first shared ledger and the second digital asset is tracked on a second shared ledger.

6. The method of claim 1, further comprising:

signing a refund transaction with the customer private key; and

transmitting a refund transaction to the counterparty with a request to refund the purchase amount of the first digital asset.

7. A method for securing the exchange of digital assets via a zero-custody switch:

receiving an order request for a non-custodial exchange of a first digital asset for a second digital asset, the first digital asset being held by a customer and the second digital asset being held by a counterparty, the request including a final payment address of the customer;

generating a cryptographic key pair including a counterparty public key and a counterparty private key;

receiving a payment address, the payment address having an encumbrance depending at least on a digital signature of at least two of the counterparty private key, a customer private key, and an oracle private key;

determining whether the payment address satisfies a funding condition; and

broadcasting one or more completion transactions based at least in part on whether the payment address satisfies the funding condition.

8. The method of claim 7, wherein broadcasting one or more completion transactions includes:

broadcasting an exchange transaction on a network of the second digital asset if the payment address satisfies the funding condition, the exchange transaction having as an output the final payment address of the customer;

outputting a release transaction, the release transaction spending funds in the payment address to a counterparty address;

signing the release transaction with the counterparty private key; and

transmitting the release transaction to an oracle, the release transaction including a request to sign the release transaction with the oracle private key.

9. The method of claim 7, further comprising:

determining that the oracle is inoperative, wherein the one or more completion transactions include a refund transaction signed by the customer private key and the counterparty private key.

10. The method of claim 7, wherein the order request for a non-custodial exchange includes a desired amount of the first digital asset and a desired amount of the second digital asset.

11. The method of claim 7, wherein the operation that receives the payment address further includes:

receiving a customer public key and an oracle public key; and

generating the encumbrance on the payment address based at least in part on the counterparty public key, the customer public key, and the oracle public key.

12. The method of claim 7, wherein the exchange transaction partially fills the order request, and further comprising:

outputting a partial refund transaction, the partial refund transaction defining a difference between a value of the exchange transaction and a request exchange amount included in the order request;

signing the partial refund transaction with the counterparty private key; and

transmitting the partial refund transaction to the oracle with a request to sign the partial refund transaction with the oracle private key.

13. The method of claim 7, further comprising:

receiving a refund transaction from the oracle pre-signed with the oracle private key, the refund transaction spending the payment address to a refund address of the customer, wherein the one or more completion transactions include the refund transaction.

14. A non-transitory computer-readable medium encoded with instructions for operating a zero-custody switch, the instructions comprising:

receiving an order request to exchange a first digital asset for a second digital asset, the order request including a final payment address of a customer and a refund address of the customer;

receiving a customer public key and a counterparty public key;

generating a key pair including a private oracle key and a public oracle key;

receiving a payment address for funding the order request, the payment address having an encumbrance;

determining whether the payment address satisfies a funding condition;

determining whether the final payment address of the customer satisfies a final payment condition; and

signing a completion transaction with the private oracle key, the completion transaction being a release transaction spending funds in the payment address to a counterparty address if the funding condition and the final payment condition are satisfied, and the completion transaction being a refund transaction spending funds in the payment address to the refund address of the customer if the final payment condition is not satisfied.

15. The non-transitory computer-readable medium of claim 14, wherein the first digital asset is tracked on a first shared ledger and the second digital asset is tracked on a second shared ledger.

16. The non-transitory computer-readable medium of claim 15, wherein the instructions further comprise:

waiting until the expiration of a race-condition period before the operation that signs the completion transaction with the oracle private key.

17. The non-transitory computer-readable medium of claim 14, wherein the non-transitory computer-readable medium is executed on a decentralized network according to consensus rules, wherein the first digital asset and the second digital asset are tracked on the decentralized network.

18. The non-transitory computer-readable medium of claim 14, wherein the instructions further comprise:

receiving a refund request from the customer to cancel the order request, the refund request including the completion transaction, the completion transaction being a refund transaction spending funds in the payment address to a customer refund address, the completion transaction further being signed by the customer private key; and

signing the refund transaction, if the final address does not satisfy the receipt condition.

19. The non-transitory computer-readable medium of claim 14, further comprising:

determining an expiration period of the order request has elapsed;

determining the final payment address of the customer does not satisfy the final payment condition; and

signing a refund transaction spending funds in the payment account to the customer refund address, wherein the encumbrance is satisfied by the expiration period and a signature the oracle private key.

20. The non-transitory computer-readable medium of claim 14, wherein the operation that receives the payment address includes generating the encumbrance on the payment address, the encumbrance being based at least in part on a digital signature of at least two of a counterparty private key, a customer private key, and the oracle private key.