

CRYPTO INTEGRATION PLATFORM

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to and benefit from United States Provisional Application No. 62/113,931, filed on February 9, 2015, entitled "CRYPTO INTEGRATION PLATFORM," which is hereby incorporated by reference in its entirety for all purposes.

TECHNICAL FIELD

[0002] Various embodiments of the present disclosure generally relate to trading. More specifically, various embodiments of the present disclosure relate to systems and methods for trading digital transactional items such as assets, liabilities, commodities, and/or currencies using distributed and cryptographic ("crypto") techniques.

BACKGROUND

[0003] Recent increasing adoption of crypto currencies (e.g., Bitcoin) worldwide creates challenges for existing trading systems. For example, market data and ownership data are stored differently. Additionally, existing trading systems use protocols for pre-trade communications and execution that are not compatible with trading systems that trade digital transactional items.

[0004] The present disclosure overcomes these and other limitations of existing trading systems, and provides other benefits as will become clearer to those skilled in the art from the following description.

SUMMARY OF THE INVENTION

[0004A] The present disclosure provides a computerized method comprising:

creating, by a computer, a first addressed account and a second addressed account for a first customer, each of the first addressed account and the second addressed account having a common customer identifier associated with the first customer;

receiving, from a remote computing device, an order for exchanging one or more digital transactional items associated with the first addressed account, wherein the order is associated with the common customer identifier;

electronically signing, with a private key associated with the first addressed account, a first transaction to transfer the one or more digital transactional items from the first addressed account to the second addressed account;

electronically signing, with the private key associated with the first addressed account, a second transaction;

verifying that the first transaction was signed with the same private key as the second transaction; and

authorizing placement of the order on a cryptographic exchange upon verifying that the first transaction was signed with the same private key as the second transaction.

[0004B] The present disclosure also provides a computerized method comprising

receiving, from a broker-dealer, a request to match a buy transaction with a sell transaction,

wherein the buy transaction includes a buy order to purchase one or more digital transactional items for an amount corresponding to a value of the one or more digital transactional items and the sell transaction includes a sell order to sell the one or more digital transactional items for the amount,

wherein the buy transaction has an associated first signature that corresponds to a first addressed account that identifies the buy order, wherein the sell transaction has an associated second signature corresponding to a second addressed account that identifies the sell order, the first addressed account being associated with a first customer and the second addressed account being associated with a second customer,

wherein the amount is associated with a third addressed account associated with the first customer and the one or more digital transactional items are associated with a fourth addressed account associated with the second customer;

mapping, by a computer, the buy transaction to the third addressed account and the sell transaction to the fourth addressed account;

sending, to the cryptographic exchange, a match request response including the first signature and the second signature to commit the buy transaction; and

transferring the one or more digital transactional items from the fourth addressed account associated with the second customer to the first addressed account associated with the first

customer and transferring the amount from the third addressed account associated with the first customer to the second addressed account associated with the second customer to settle and clear the buy transaction and the sell transaction.

[0004C] The present disclosure further provides a cryptographic integration system, comprising:

- at least one processor; and

- at least one computer readable storage medium having instructions stored thereon, which when executed by the at least one processor causes the cryptographic integration system to:

- receive an order to execute a trade for one or more digital transactional items associated with a first addressed account, wherein the order, the first addressed account, and a second addressed account are associated with a common identifier;

- generate a first transaction to transfer the one or more digital transactional items from the first addressed account to the second addressed account;

- generate a second transaction that includes the order;

- verify that the first transaction was authorized by a same party as the second transaction; and

- authorize placement of the order on a cryptographic exchange after verifying that the first transaction was authorized by the same party as the second transaction.

[0004C] The present disclosure further provides a non-transitory computer-readable storage medium including a set of instructions that, when executed by one or more processors, cause a machine to:

- create a first addressed account and a second addressed account for a first customer, each of the first addressed account and the second addressed account having a common customer identifier associated with the first customer;

- receive an order for exchanging one or more digital transactional items associated with the first addressed account, wherein the order is associated with the common customer identifier;

- electronically sign, with a private key associated with the first addressed account, a first transaction to transfer the one or more digital transactional items from the first addressed account to the second addressed account;

- electronically sign, with the private key associated the first addressed account, a second transaction;

verify that the first transaction was signed with the same private key as the second transaction; and

authorize placement of the order on a cryptographic exchange upon verifying that the first transaction was signed with the same private key as the second transaction.

[0004C] The present disclosure further provides a non-transitory computer-readable storage medium including a set of instructions that, when executed by one or more processors, cause a machine to:

receive, from a broker-dealer, a request to match a buy transaction with a sell transaction, wherein the buy transaction includes a buy order to purchase one or more digital transactional items for an amount corresponding to a value of the one or more digital transactional items and the sell transaction includes a sell order to sell the one or more digital transactional items for the amount,

wherein the buy transaction has an associated first signature that corresponds to a first addressed account that identifies the buy order, wherein the sell transaction has an associated second signature corresponding to a second addressed account that identifies the sell order, the first addressed account being associated with a first customer and the second addressed account being associated with a second customer,

wherein the amount is associated with a third addressed account associated with the first customer and the one or more digital transactional items are associated with a fourth addressed account associated with the second customer;

map the buy transaction to the third addressed account and the sell transaction to a fourth addressed account;

send, to the cryptographic exchange, a match request response including the first signature and the second signature to commit the buy transaction; and

transfer the one or more digital items from the fourth addressed account associated with the second customer to the first addressed account associated with the first customer and transfer the amount from the third addressed account associated with the first customer to the second addressed account associated with the second customer to settle and clear the buy transaction and the sell transaction.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] Embodiments of the present disclosure will be described and explained through the use of the accompanying drawings in which:

[0006] Fig. 1 illustrates an example of a network-based operating environment in accordance with various embodiments of the disclosure;

DETAILED DESCRIPTION

[0020] Various embodiments of the present disclosure generally relate to trading digital transactional items, more particularly digital assets, such as securities. More specifically, various embodiments of the present disclosure relate to systems and methods for trading digital securities using distributed and cryptographic techniques, and, in particular, a Crypto Integration Platform. The Crypto Integration Platform receives orders to trade digital transactional items such as digital assets, liabilities, commodities, and/or currencies (e.g., digital securities, digital interests in securities, crypto currencies) for other digital transactional items such as digital representations of funds (e.g., tokens, cash, cash equivalents such as crypto currencies) on a cryptographic ("crypto") exchange (i.e., an exchange that trades digital transactional items) from broker-dealers and translates the orders into crypto orders.

[0021] The Crypto Integration Platform aggregates market information from the crypto exchanges and serves as a router to locate the best price in the crypto market for the digital asset or liability involved in the transaction. Prior to matching orders, the Crypto Integration Platform secures both the digital transactional items (i.e., the funds for a buy order and the digital assets or liabilities for a sell order) and cryptographically signs the transactions. Once a potential matching order has been located, the Crypto Integration Platform verifies that the funds and the digital assets/liabilities are available for trade (e.g., associated with addressed accounts owned by the buyer and the seller) and clears and settles the transaction instantaneously by associating the funds and digital assets or liabilities with corresponding addressed accounts.

[0022] Benefits of the Crypto Integration Platform include guaranteed settlement, transparency of ownership and easy money movement, and secure settlements. Cryptographically signing the transactions ensures authentication, authorization, and provenance.

[0023] The Crypto Integration Platform provides, among other things, an interface between legacy trading systems and crypto exchanges that trade digital transactional items. In doing so, the Crypto Integration Platform takes a protocol for trading and communication between broker-dealers, Alternative Trading Systems

Adapter 215 also integrates new customers by storing a customer identifier provided by the broker-dealer and generating two separate key pairs. Each key pair has one private key and one public key. The two parts of the key pair are mathematically linked. The public key of a key pair may be published without compromising security, whereas the private key of a key pair must not be revealed to anyone not authorized to read messages or perform digital signatures.

[0044] The two key pairs are used to create two addressed accounts associated with the customer identifier. The addressed accounts may be referred to as "wallets." Both wallets represent digital accounts. The first wallet, referred to at times, herein as the customer portfolio wallet, stores digital transactional items such as digital assets and liabilities (e.g., digital shares of stocks) and digital funds (e.g., digitized dollars, tokens, crypto currency). In some embodiments, the customer associated with the customer identifier owns the key pair for the wallet, but authorizes Crypto Adapter 215 to use the key pair to complete transactions on behalf of the customer. In other embodiments, Crypto Adapter 215 or a third party owns the customer portfolio wallet. The second wallet, referred to at times herein as the customer committed wallet, stores digital transactional items that the customer has placed in buy or sell orders that have not yet been completed (e.g., "committed" assets or funds). Crypto Adapter 215 either owns the keys for the customer committed wallet or is authorized to use the keys to the customer committed wallet. In some embodiments, a parent wallet may be created that includes many different customer portfolio wallet and customer committed wallet keys. The parent wallet may include keys for different public ledgers thereby providing one master account for a brokerdealer.

[0045] Crypto Adapter 215 can receive a request from a broker-dealer to obtain the balance of the wallets. Using the customer identifier, Crypto Adapter 215 can identify the correct customer portfolio wallet and customer committed wallet. Then, Crypto Adapter 215 can use the corresponding public key for the customer portfolio wallet and the customer committed wallet to obtain the balance for each wallet from one or more crypto ledgers.

[0046] Crypto Adapter 215 can receive a FIX order message (or similar message) that includes a buy, sell, or cancel order associated with a customer identifier from

CLAIMS

What is claimed is

1. A computerized method comprising:
 - creating, by a computer, a first addressed account and a second addressed account for a first customer, each of the first addressed account and the second addressed account having a common customer identifier associated with the first customer;
 - receiving, from a remote computing device, an order for exchanging one or more digital transactional items associated with the first addressed account, wherein the order is associated with the common customer identifier;
 - electronically signing, with a private key associated with the first addressed account, a first transaction to transfer the one or more digital transactional items from the first addressed account to the second addressed account;
 - electronically signing, with the private key associated with the first addressed account, a second transaction;
 - verifying that the first transaction was signed with the same private key as the second transaction; and
 - authorizing placement of the order on a cryptographic exchange upon verifying that the first transaction was signed with the same private key as the second transaction.
2. The computerized method of claim 1, wherein the second addressed account is associated with a second key pair which includes a second public key and a second private key.
3. The computerized method of claim 1, further comprising:
 - receiving confirmation, from a distributed ledger, that the one or more digital transactional items associated with the order are associated with the first addressed account by using the first public key; and

upon receiving the confirmation that the one or more digital transactional items associated with the order are associated with the first addressed account, creating the first transaction and the second transaction.

4. The computerized method of claim 1, further comprising:
communicating, to a distributed ledger, a balance of the first addressed account and the second addressed account.

5. The computerized method of claim 1, wherein the order is an order to purchase a digital asset or a digital liability, the computerized method further comprising:

receiving, from the remote computing device, information indicating that funds are available to purchase the digital asset or the digital liability, wherein the one or more digital transactional items is a digital representation of the funds; and

associating the digital representation of the funds with the first addressed account as the one or more digital transactional items.

6. The computerized method of claim 1, wherein the order is an order to sell the one or more digital transactional items, wherein the one or more digital transactional items is one or more digital assets or one or more digital liabilities, the computerized method further comprising:

receiving, from the remote computing device, information indicating that assets corresponding to the one or more digital assets or liabilities corresponding to the one or more digital liabilities are available to sell.

7. The computerized method of claim 1, further comprising:

creating a third addressed account, wherein the third addressed account includes a first key pair associated with the first addressed account and a second key pair associated with the second addressed account.

8. The computerized method of claim 1, further comprising:

creating the first transaction, wherein the first transaction includes at least one of: the one or more digital transactional items, the common customer identifier, and a public key of the second addressed account;

creating a hash of the first transaction; and

creating the second transaction, wherein the second transaction includes at least one of: a type of the order, the common customer identifier, a public key of the second addressed account, and the hash of the first transaction.

9. The computerized method of claim 1, further comprising:
sending the first transaction to the cryptographic exchange; and
sending the second transaction to an alternative trading system.

10. The computerized method of claim 9, further comprising:
receiving a notification that the order has been matched to a second order on the cryptographic exchange; and
creating an execution report.

11. The computerized method of claim 1, wherein the first addressed account is a customer portfolio account, wherein the second addressed account is a customer committed account.

12. The computerized method of claim 1, wherein the first transaction includes at least one of: funds in an amount corresponding to a value of the first transaction or a representation of the funds in the amount corresponding to the value of the first transaction and a public key of the first addressed account, and wherein the second transaction includes at least one of: a public key of the second addressed account, a type of the order, the common customer identifier, a public key of the second addressed account, and a hash of the first transaction.

13. A computerized method comprising
receiving, from a broker-dealer, a request to match a buy transaction with a sell transaction,

wherein the buy transaction includes a buy order to purchase one or more digital transactional items for an amount corresponding to a value of the one or more digital transactional items and the sell transaction includes a sell order to sell the one or more digital transactional items for the amount,

wherein the buy transaction has an associated first signature that corresponds to a first addressed account that identifies the buy order, wherein the sell transaction has an associated second signature corresponding to a second addressed account that identifies the sell order, the first addressed account being associated with a first customer and the second addressed account being associated with a second customer,

wherein the amount is associated with a third addressed account associated with the first customer and the one or more digital transactional items are associated with a fourth addressed account associated with the second customer;

mapping, by a computer, the buy transaction to the third addressed account and the sell transaction to the fourth addressed account;

sending, to the cryptographic exchange, a match request response including the first signature and the second signature to commit the buy transaction; and

transferring the one or more digital transactional items from the fourth addressed account associated with the second customer to the first addressed account associated with the first customer and transferring the amount from the third addressed account associated with the first customer to the second addressed account associated with the second customer to settle and clear the buy transaction and the sell transaction.

14. The computerized method of claim 13, further comprising:

receiving confirmation, from a distributed ledger, that the amount is associated with the third addressed account and that the one or more digital transactional items are associated with the fourth addressed account prior to sending the match request response.

15. The computerized method of claim 13, wherein the one or more digital transactional items include one or more of digital assets or digital liabilities, wherein the amount includes an amount of currency, cryptographic currency, or a representation of the currency or the cryptographic currency corresponding to a value of the one or more digital transactional items.
16. The computerized method of claim 13, further comprising:
publishing, to a remote computing device, results of settling and clearing the buy transaction and the sell transaction.
17. The computerized method of claim 13, wherein the first signature is a private key associated with the first addressed account, wherein the second signature is a private key associated with the second addressed account.
18. The computerized method of claim 13, wherein:
the first addressed account is a customer portfolio account associated with the first customer,
the second addressed account is a customer portfolio account associated with the second customer,
the third addressed account is a customer committed account associated with the first customer, and
the fourth addressed account is a customer committed account associated with the second customer.
19. A cryptographic integration system, comprising:
at least one processor; and
at least one computer readable storage medium having instructions stored thereon, which when executed by the at least one processor causes the cryptographic integration system to:
receive an order to execute a trade for one or more digital transactional items associated with a first addressed account, wherein the order, the first addressed account, and a second addressed account are associated with a common identifier;

generate a first transaction to transfer the one or more digital transactional items from the first addressed account to the second addressed account;
generate a second transaction that includes the order;
verify that the first transaction was authorized by a same party as the second transaction; and
authorize placement of the order on a cryptographic exchange after verifying that the first transaction was authorized by the same party as the second transaction.

20. The cryptographic integration system of claim 19, wherein the first transaction is authorized by the same party as the second transaction when the first transaction and the second transaction are signed by a same key.

21. The cryptographic integration systems of claim 20, wherein the key is a private key of the first addressed account, and wherein the second transaction includes a hash of the first transaction.

22. The cryptographic integration system of claim 19, wherein the instructions, which when executed by the at least one processor further cause the cryptographic integration system to:
receive, from the cryptographic exchange, a request to match the order with a second order, wherein the second order is associated with a second identifier; and
transfer the one or more digital transactional items to an addressed account associated with the second identifier and transfer one or more other digital transactional items into the first addressed account to settle and clear the order.

23. The cryptographic integration system of claim 19, further comprising:
a cryptographic adapter component configured to:
send the first transaction to the cryptographic exchange; and
send the second transaction to an alternative trading system.

24. A non-transitory computer-readable storage medium including a set of instructions that, when executed by one or more processors, cause a machine to:

- create a first addressed account and a second addressed account for a first customer, each of the first addressed account and the second addressed account having a common customer identifier associated with the first customer;

- receive an order for exchanging one or more digital transactional items associated with the first addressed account, wherein the order is associated with the common customer identifier;

- electronically sign, with a private key associated with the first addressed account, a first transaction to transfer the one or more digital transactional items from the first addressed account to the second addressed account;

- electronically sign, with the private key associated the first addressed account, a second transaction;

- verify that the first transaction was signed with the same private key as the second transaction; and

- authorize placement of the order on a cryptographic exchange upon verifying that the first transaction was signed with the same private key as the second transaction.

25. A non-transitory computer-readable storage medium including a set of instructions that, when executed by one or more processors, cause a machine to:

- receive, from a broker-dealer, a request to match a buy transaction with a sell transaction,

- wherein the buy transaction includes a buy order to purchase one or more digital transactional items for an amount corresponding to a value of the one or more digital transactional items and the sell transaction includes a sell order to sell the one or more digital transactional items for the amount,

- wherein the buy transaction has an associated first signature that corresponds to a first addressed account that identifies the buy order, wherein the sell transaction has an associated second signature corresponding to a second addressed account that identifies the sell order, the first addressed account being associated with a first customer and the second addressed account being associated with a second customer,

wherein the amount is associated with a third addressed account associated with the first customer and the one or more digital transactional items are associated with a fourth addressed account associated with the second customer;

map the buy transaction to the third addressed account and the sell transaction to a fourth addressed account;

send, to the cryptographic exchange, a match request response including the first signature and the second signature to commit the buy transaction; and

transfer the one or more digital items from the fourth addressed account associated with the second customer to the first addressed account associated with the first customer and transfer the amount from the third addressed account associated with the first customer to the second addressed account associated with the second customer to settle and clear the buy transaction and the sell transaction.