

asset exchange infrastructure, an order book is not visible to all traders, which makes the order book dependent on for-profit matchmakers and therefore susceptible to manipulation. It is desirable to ensure that an order matching process is free of manipulation, while keeping a trader's order information (e.g., a trader's identity, a price, and a quantity) private.

SUMMARY

[0005] In one embodiment, there is provided a computer-implemented method for transaction matching, the method comprising: receiving one or more transactions; determining at least one of a match between the one or more transactions and a stored data structure or a match between one and another of the one or more transactions; sending, to a blockchain system, a request for validation of a determination result; and updating the stored data structure in response to the validation of the determination result by the blockchain system, wherein sending, to the blockchain system, the request for validation of the determination result further comprises: uploading, to the blockchain system, at least one of: a range proof of a price of matched transactions; a range proof of a quantity of the matched transactions; an equal relationship between two quantities of the matched transactions; or a linear relationship between a plurality of quantities of the matched transactions, wherein: each of the range proof of the price of the matched transactions and the range proof of the quantity of the matched transactions is based on a zero-knowledge range proof, and each of the equal relationship between two quantities of the matched transactions and the linear relationship between the plurality of quantities of the matched transactions is based on a zero-knowledge proof of

knowledge of a discrete logarithm.

[0006] In another embodiment, there is provided a device for transaction matching, the device comprising: one or more processors; and one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to: receive one or more transactions; determine at least one of a match between the one or more transactions and a stored data structure or a match between one and another of the one or more transactions; send, to a blockchain system, a request for validation of a determination result; and update the stored data structure in response to the validation of the determination result by the blockchain system, wherein sending, to the blockchain system, the request for validation of the determination result further comprises: uploading, to the blockchain system, at least one of: a range proof of a price of matched transactions; a range proof of a quantity of the matched transactions; an equal relationship between two quantities of the matched transactions; or a linear relationship between a plurality of quantities of the matched transactions, wherein: each of the range proof of the price of the matched transactions and the range proof of the quantity of the matched transactions is based on a zero-knowledge range proof, and each of the equal relationship between two quantities of the matched transactions and the linear relationship between the plurality of quantities of the matched transactions is based on a zero-knowledge proof of knowledge of a discrete logarithm.

[0006a] In another embodiment, there is provided an apparatus for transaction matching, the apparatus comprising a plurality of modules to: receive one or more transactions; determine at least one of a match between the one or more transactions

and a stored data structure or a match between one and another of the one or more transactions; send, to a blockchain system, a request for validation of a determination result; and update the stored data structure in response to the validation of the determination result by the blockchain system, wherein sending, to the blockchain system, the request for validation of the determination result further comprises: uploading, to the blockchain system, at least one of: a range proof of a price of matched transactions; a range proof of a quantity of the matched transactions; an equal relationship between two quantities of the matched transactions; or a linear relationship between a plurality of quantities of the matched transactions, wherein: each of the range proof of the price of the matched transactions and the range proof of the quantity of the matched transactions is based on a zero-knowledge range proof, and each of the equal relationship between two quantities of the matched transactions and the linear relationship between the plurality of quantities of the matched transactions is based on a zero-knowledge proof of knowledge of a discrete logarithm.

[0007] In another embodiment, there is provided a non-transitory computer-readable medium having stored therein instructions that, when executed by a processor of a device, cause the device to perform a method for transaction matching, the method comprising: receiving one or more transactions; determining at least one of a match between the one or more transactions and a stored data structure or a match between one and another of the one or more transactions; sending, to a blockchain system, a request for validation of a determination result; and updating the stored data structure in response to the validation of the determination result by the blockchain system, wherein sending, to the blockchain system, the request for validation of the determination result

further comprises: uploading, to the blockchain system, at least one of: a range proof of a price of matched transactions; a range proof of a quantity of the matched transactions; an equal relationship between two quantities of the matched transactions; or a linear relationship between a plurality of quantities of the matched transactions, wherein: each of the range proof of the price of the matched transactions and the range proof of the quantity of the matched transactions is based on a zero-knowledge range proof, and each of the equal relationship between two quantities of the matched transactions and the linear relationship between the plurality of quantities of the matched transactions is based on a zero-knowledge proof of knowledge of a discrete logarithm.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate embodiments. In the following description, which refers to the drawings, the same numbers in different drawings represent the same or similar elements unless otherwise represented.

[0009] FIG. 1 is a schematic diagram of a blockchain system, according to an embodiment.

[0010] FIG. 2 is a schematic diagram of a system for order matching, according to an embodiment.

[0011] FIG. 3 is a schematic diagram of a device for order matching, according to an embodiment.

[0012] FIG. 4 is a schematic diagram illustrating an order book, according to an embodiment.

Claims

1. A computer-implemented method for transaction matching, comprising:
 - receiving one or more transactions;
 - determining at least one of a match between the one or more transactions and a stored data structure or a match between one and another of the one or more transactions;
 - sending, to a blockchain system, a request for validation of a determination result; and
 - updating the stored data structure in response to the validation of the determination result by the blockchain system,wherein sending, to the blockchain system, the request for validation of the determination result further comprises:
 - uploading, to the blockchain system, at least one of:
 - a range proof of a price of matched transactions;
 - a range proof of a quantity of the matched transactions;
 - an equal relationship between two quantities of the matched transactions; or
 - a linear relationship between a plurality of quantities of the matched transactions,wherein:
 - each of the range proof of the price of the matched transactions and the range proof of the quantity of the matched transactions is based on a zero-knowledge range proof, and
 - each of the equal relationship between two quantities of the matched transactions and the linear relationship between the plurality of quantities of

the matched transactions is based on a zero-knowledge proof of knowledge of a discrete logarithm.

2. The method of claim 1, wherein the one or more transactions are received from a broadcast by the blockchain system or a broadcast by another blockchain system different from the blockchain system.

3. The method of claim 1, wherein the one or more transactions are received from one or more user interface devices.

4. The method of any preceding claim, wherein the one or more transactions comprise at least one of:

one or more buy orders;

one or more sell orders; or

one or more buy orders and one or more sell orders.

5. The method of any preceding claim, wherein each of the received one or more transactions includes a transaction type and at least one of: a commitment of a price, a commitment of a quantity, a price encrypted by a cryptographic key, a quantity encrypted by the cryptographic key, a random number that is used to generate the commitment of the price and encrypted by the cryptographic key, or a random number that is used to generate the commitment of the quantity and encrypted by the cryptographic key.

6. The method of claim 5, wherein the commitment of the price is a Pedersen commitment of the price and the commitment of the quantity is a Pedersen commitment of the quantity.

7. The method of any preceding claim, wherein determining at least one of the match between the one or more transactions and the stored data structure or the match between one and another of the one or more transactions is performed based on at least one price included in the one or more transactions.

8. The method of any of claims 1 to 6, wherein determining at least one of the match between the one or more transactions and the stored data structure or the match between one and another of the one or more transactions is performed based on:

one or more lowest prices of one or more sell orders included in the stored data structure; or

one or more highest prices of one or more buy orders included in the stored data structure.

9. The method of any preceding claim, further comprising:

verifying, on one or more nodes of the blockchain system, validity of the determination result based on the request for validation of the determination result.

10. A device for matching one or more transactions, comprising:

one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 9.

11. An apparatus for matching one or more transactions, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 9.

12. A non-transitory computer-readable medium having stored therein instructions that, when executed by a processor of a device, cause the device to perform the method of any of claims 1 to 9.