

BLOCKCHAIN-BASED REMITTANCE PATH MANAGEMENT

TECHNICAL FIELD

[0001] The present disclosure relates to the field of blockchain technologies, and in particular, to a method and an apparatus for managing a remittance path based on a blockchain.

5

BACKGROUND

[0002] Currently, a blockchain can serve a remittance transaction by executing a remittance transaction contract. When a remittance initiator needs to initiate a target remittance transaction, the remittance initiator needs to first query an available remittance path of a participant of the target remittance transaction by using a centralized system of a financial platform. If the available remittance path identified by the remittance initiator matches a remittance path needed by the target remittance transaction, a user can initiate the target remittance transaction on the blockchain by invoking a remittance transaction contract. In this case, the blockchain can record a transaction result of the target remittance transaction by executing the remittance transaction contract.

10

[0003] In other words, the available remittance path of the participant of the target remittance transaction is maintained using the centralized system. In some cases, when the remittance initiator queries the available remittance path by using the centralized system, the centralized system causes an error in the maintained available remittance path due to a system error, and consequently, returns an incorrect result to the remittance initiator, degrading user experience. For example, the available remittance path of the participant originally matches the remittance path needed by the target remittance transaction. However, due to an error in the centralized system, the maintained available remittance path of the participant is incorrect. In this case, the centralized system records the available remittance path of the participant as an unavailable remittance path, and returns an incorrect result such as "mismatch or no available remittance path" to the remittance initiator. Consequently, the remittance initiator cannot initiate the target remittance transaction, degrading user experience.

15

20

25

SUMMARY

[0004] In view of this, an embodiment of the present disclosure is intended to provide a method

for managing a remittance path based on a blockchain, so as to reduce a possibility that an error occurs when a centralized system maintains an available remittance path, thereby improving user experience.

[0005] According to a first aspect, a method for managing a remittance path based on a blockchain is provided. The blockchain stores a first smart contract, the first smart contract is used to manage an available remittance path of at least one participant among a plurality of participants of a target remittance transaction, the available remittance path of the at least one participant is used to indicate an available remittance path that can be provided by the at least one participant for the target remittance transaction, and the at least one participant includes a first participant. The method includes: receiving a first invoking request of the first smart contract from the first participant, where the first invoking request is used to set an available remittance path of the first participant; and setting the available remittance path of the first participant in the first smart contract based on the first invoking request.

[0006] According to a second aspect, a method for managing a remittance path based on a blockchain is provided. The blockchain stores a first smart contract, the first smart contract is used to manage an available remittance path of at least one participant among a plurality of participants of a target remittance transaction, the available remittance path of the at least one participant is used to indicate an available remittance path that can be provided by the at least one participant for the target remittance transaction, the at least one participant includes a first participant, and the method is applied to the first participant. The method includes: obtaining an available remittance path of the first participant; and sending a first invoking request of the first smart contract to the blockchain, where the first invoking request is used to set the available remittance path of the first participant.

[0007] According to a third aspect, an apparatus for managing a remittance path based on a blockchain is provided. The blockchain stores a first smart contract, the first smart contract is used to manage an available remittance path of at least one participant among a plurality of participants of a target remittance transaction, the available remittance path of the at least one participant is used to indicate an available remittance path that can be provided by the at least one participant for the target remittance transaction, and the at least one participant includes a first participant. The apparatus includes: a receiving module, configured to receive a first invoking request of the first smart contract from the first participant, where the first invoking request is used to set an available remittance path of the first participant; and a processing module, configured to set the available remittance path of the first participant in the first smart contract based on the first invoking request.

[0008] According to a fourth aspect, an apparatus for managing a remittance path based on a blockchain is provided. The blockchain stores a first smart contract, the first smart contract is used

to manage an available remittance path of at least one participant among a plurality of participants of a target remittance transaction, the available remittance path of the at least one participant is used to indicate an available remittance path that can be provided by the at least one participant for the target remittance transaction, the at least one participant includes a first participant, and the apparatus is applied to the first participant. The apparatus includes: an obtaining module, configured to obtain an available remittance path of the first participant; and a sending module, configured to send a first invoking request of the first smart contract to the blockchain, where the first invoking request is used to set the available remittance path of the first participant.

[0009] According to a fifth aspect, an apparatus for managing a remittance path based on a blockchain is provided, including a memory and a processor, where the memory stores executable code, and the processor is configured to execute the executable code to implement the method according to the first aspect or the second aspect.

[0010] According to a sixth aspect, a computer-readable storage medium is provided, where the computer-readable storage medium stores executable code, and the executable code is executed to implement the method according to the first aspect or the second aspect.

[0011] According to a seventh aspect, a computer program product is provided, including executable code, and the executable code is executed to implement the method according to the first aspect or the second aspect.

[0012] According to the solutions in the embodiments of the present disclosure, an available remittance path of a participant of a target remittance transaction is maintained on a blockchain by using a first smart contract, so that the participant serving as a user of the blockchain can autonomously maintain the available remittance path by invoking the first smart contract. This avoids an incorrect available remittance path of the participant due to an error in the centralized system in a conventional solution of maintaining the available remittance path of the participant by using the centralized system, thereby helping reduce a possibility that an error occurs when the centralized system maintains the available remittance path, and improving user experience.

BRIEF DESCRIPTION OF DRAWINGS

[0013] FIG. 1 is a schematic diagram of an architecture of a blockchain to which an embodiment of the present disclosure is applicable;

[0014] FIG. 2 is a schematic flowchart of initiating a target remittance transaction by a capitalist A;

[0015] FIG. 3 is a schematic flowchart of a method for managing a remittance path based on a blockchain according to an embodiment of the present disclosure;

[0016] FIG. 4 is a schematic flowchart of a process of updating a first smart contract according to an embodiment of the present disclosure;

[0017] FIG. 5 is a schematic flowchart of a process of using a first smart contract according to an embodiment of the present disclosure;

5 [0018] FIG. 6 is a schematic flowchart of a process of querying a first smart contract according to an embodiment of the present disclosure;

[0019] FIG. 7 is a schematic structural diagram of an apparatus for managing a remittance path based on a blockchain according to an embodiment of the present disclosure;

10 [0020] FIG. 8 is a schematic structural diagram of an apparatus for managing a remittance path based on a blockchain according to another embodiment of the present disclosure;

[0021] FIG. 9 is a schematic structural diagram of an apparatus for managing a remittance path based on a blockchain according to still another embodiment of the present disclosure; and

[0022] FIG. 10 is a schematic structural diagram of an apparatus for managing a remittance path based on a blockchain according to still another embodiment of the present disclosure.

15

DESCRIPTION OF EMBODIMENTS

[0023] The following clearly and comprehensively describes technical solutions in embodiments of the present disclosure with reference to accompanying drawings in the embodiments of the present disclosure. Clearly, the described embodiments are merely some rather than all of the embodiments of the present disclosure.

20 [0024] To facilitate understanding of the solutions of the present disclosure, the following first describes, with reference to FIG. 1, a blockchain architecture to which the present disclosure is applicable, and some related concepts.

[0025] Blockchain architecture.

25 [0026] FIG. 1 is a schematic diagram of an architecture of a blockchain to which an embodiment of the present disclosure is applicable. The architecture 100 shown in FIG. 1 includes a blockchain node 110 and a user node 120.

30 [0027] The blockchain is a typical distributed collaboration system, in which a plurality of parties jointly maintain an increasing distributed data record. Data of these records is protected in terms of content and time series by using a cryptographic technology, so that it is difficult for any party to tamper with, repudiate, or falsify the data.

[0028] In the blockchain, the data (e.g., packaged transaction data and transaction execution results) can be encapsulated in the form of a block. Blocks can be linked to each other by forward applications to form a "chain", that is, a blockchain. In some implementations, each block records

basic data such as a hash value of a previous block, a transaction set in the local block, and a hash of the local block.

[0029] Usually, the user node 120 of the blockchain can communicate with the blockchain node 110 by using a client. In some cases, the user node 120 can send the data that needs to be stored to one or more associated blockchain nodes 110 by committing a transaction. The transaction may be understood as a transaction request on the blockchain, and is used to carry a structure of specific service operation data. All change operations with respect to a world state on the blockchain can be completed based on transactions.

[0030] Correspondingly, after verifying the validity of the data, the blockchain node 110 can broadcast the data to each blockchain node 110 in a network-wide broadcast manner. In this way, each blockchain node 110 records full and consistent data.

[0031] For example, in the scenario of performing a remittance transaction in this embodiment of the present disclosure, the blockchain node 110 may be a node that can perform a remittance-related function, such as recording a transaction status of the remittance transaction.

Correspondingly, the user node 120 may include a user node located at a remittance initiator, for example, a user node 122 of the capitalist A. The user node 120 may further include a user node of a remittance institution that makes remittance, for example, a user node 121 of a remittance bank. The user node 120 may further include a user node of a payee institution that receives remittance, for example, a user node 123 of a payee bank.

[0032] In some implementations, the blockchain node 110 may be a server or another device that has a computing capability. The user node 120 may be a server, a mobile terminal, or another device that has a computing capability.

[0033] Smart contract.

[0034] A smart contract is a set of commitments defined digitally, including a protocol on which contract participants can execute these commitments. Alternatively, the smart contract may be understood as a segment of program deployed on a computer system. When a trigger condition of the smart contract is met, the smart contract can be automatically executed.

[0035] The emergence of the blockchain provides technical support for implementing the smart contract. The smart contract is digitally written into the blockchain, and a feature of the blockchain technology ensures that an entire process of storing, reading, and executing the smart contract is transparent, traceable, and tamper-resistant. In addition, a state machine system can be constructed by using a consensus algorithm that comes with the blockchain, so that the smart contract can run efficiently.

[0036] In some implementations, the user can invoke a smart contract by committing a

transaction to a blockchain system, set data recorded in the smart contract, and store the set smart contract in the blockchain. Correspondingly, after a specific condition of the smart contract is triggered, the blockchain node can execute the smart contract, and record an execution result of the smart contract and an execution status of the smart contract.

5 **[0037]** Currently, a blockchain can serve a remittance transaction by executing a remittance transaction contract. When a remittance initiator needs to initiate a target remittance transaction, the remittance initiator needs to first query an available remittance path of a participant of the target remittance transaction by using a centralized system of a financial platform. The available remittance path may be understood as a path between a payer and a payee that can perform the remittance transaction. If the available remittance path identified by the remittance initiator matches a remittance path needed by the target remittance transaction, a user can initiate the target remittance transaction on the blockchain by invoking a remittance transaction contract. In this case, the blockchain can record a transaction result of the target remittance transaction by executing the remittance transaction contract.

15 **[0038]** With reference to FIG. 2, the following describes a process of initiating a target remittance transaction by using an example in which a remittance initiator serving as a capitalist A initiates the target remittance transaction. It is assumed that the capitalist A needs to perform a target remittance transaction with a capitalist B, and that a remittance path needed by the target remittance transaction is remittance made by a remittance institution A to a remittance institution B. In addition, the centralized system records an available remittance path of the remittance institution A.

20 **[0039]** In step S210, the capitalist A needs to send a query request to the centralized system to query the available remittance path of the remittance institution A.

[0040] In step S220, if the remittance path from the remittance institution A to the remittance institution B is not recorded in the available remittance path of the remittance institution A, that is, the available remittance path of the remittance institution A does not match the remittance path needed by the target remittance transaction, the capitalist A does not initiate the target remittance transaction to the blockchain.

[0041] In step S230, if the remittance path from the remittance institution A to the remittance institution B is recorded in the available remittance path of the remittance institution A, that is, the available remittance path of the remittance institution A matches the remittance path needed by the target remittance transaction, the capitalist A can record, by invoking the remittance transaction contract in the blockchain, a transaction status of the target remittance transaction that is executed off the chain. The above-mentioned transaction status includes: waiting for confirmation by the other party, a transaction success, a transaction failure, and the like.

[0042] In step S240, the blockchain executes the remittance transaction contract to record the transaction status of the target remittance transaction executed off the chain.

[0043] However, as described above, the available remittance path of the participant of the target remittance transaction is maintained using the centralized system. In some cases, when the remittance initiator queries the available remittance path by using the centralized system, the centralized system causes an error in the maintained available remittance path due to a system error, and consequently, returns an incorrect result to the remittance initiator. For example, the available remittance path of the participant originally matches the remittance path needed by the target remittance transaction. However, due to an error in the centralized system, the maintained available remittance path of the participant is incorrect. In this case, the centralized system records the available remittance path of the participant as an unavailable remittance path, and returns an incorrect result such as "mismatch or no available remittance path" to the remittance initiator. Consequently, the remittance initiator cannot initiate the target remittance transaction, degrading user experience.

[0044] In addition, due to a possibility that the centralized system may behave maliciously, maintaining the available remittance path of the participant through the centralized system may reduce security of the available remittance path.

[0045] Therefore, to avoid the above-mentioned problem, the present disclosure provides a method for managing a remittance path based on a blockchain. To be specific, the first smart contract is used on the blockchain to maintain the available remittance path of the participant, so that the participant serving as a user of the blockchain can autonomously maintain the available remittance path by invoking the first smart contract, thereby helping reduce a possibility that an error occurs when the centralized system maintains the available remittance path, and improving user experience.

[0046] In addition, maintaining the available remittance path of the participant by using the first smart contract on the blockchain helps improve security of the available remittance path.

[0047] With reference to FIG. 3, the following describes a method for managing a remittance path based on a blockchain according to an embodiment of the present disclosure. For ease of understanding, a first smart contract in this embodiment of the present disclosure is first described.

[0048] The first smart contract is used to manage an available remittance path of at least one participant among a plurality of participants of a target remittance transaction. The available remittance path of the at least one participant is used to indicate an available remittance path that can be provided by the at least one participant for the target remittance transaction. Therefore, the first smart contract may also be referred to as a "remittance path management contract".

[0049] It is assumed that a remittance path needed by the target remittance transaction is a remittance transaction from bank A to bank B. In other words, the plurality of participants of the target remittance transaction include bank A and bank B. Table 1 shows a possible implementation in which the first smart contract records the available remittance path in this embodiment of the present disclosure.

Table 1

Available remittance path of a participant	
User address	Remittance path list
Bank A	Bank A - bank B, bank A branch 1 - bank A branch 3
Bank B	Bank B - bank A, bank B branch 2 - bank B branch 3, bank B - bank C

[0050] Referring to Table 1, the first smart contract records available remittance paths of bank A and bank B. The available remittance paths of bank A include a remittance path between bank A and bank B, and a remittance path between bank A branch 1 and bank A branch 2. The available remittance paths of bank B include the remittance path between bank B and bank A, a remittance path between bank B branch 2 and bank B branch 3, and a remittance path between bank B and bank C.

[0051] It should be noted that the above-mentioned available remittance path is used to indicate a path that can be used for the remittance transaction, and is not used to limit a remittance direction when the remittance transaction is executed. For example, the available remittance path "bank A - bank B" can be used to indicate a remittance transaction between bank A and bank B. To be specific, remittance can be made from bank A to bank B or from bank B to bank A.

[0052] In addition, the first smart contract can further record an available remittance path of another institution, for example, can record an available remittance path of bank D. This is not limited in this embodiment of the present disclosure.

[0053] In some cases, the available remittance path may impose a limitation on a currency type used for the remittance. For example, for the available remittance path "bank A - bank B", the available remittance path supports only a remittance mode of currency type 1 (e.g., RMB). In this way, the first smart contract can further record a currency type supported by each available remittance path. For example, the first smart contract can record an available remittance path in the format of "bank A - bank B - currency type". Certainly, for an available remittance path that imposes no limitation on the currency type, the currency type supported by the available remittance path may not be recorded. This is not limited in this embodiment of the present disclosure.

[0054] To facilitate query of the first smart contract, a query interface can be set for the first smart contract, so that another user of the blockchain can query, by using the query interface, an available remittance path recorded in the first smart contract. In addition, to facilitate updating of the first smart contract, an update interface can be further set for the first smart contract. In this way,
5 a participant can invoke the first smart contract by using the update interface, so as to update the available remittance path recorded in the first smart contract. The processes of querying and updating the first smart contract are described below with reference to FIG. 4 to FIG. 6. For brevity, details are not described herein again.

[0055] In addition, a process of creating the first smart contract is not limited in the present
10 disclosure. The first smart contract can be created and deployed in a blockchain by a provider of the blockchain, so that a user (for example, a participant of the above-mentioned target remittance transaction) of the blockchain invokes the first smart contract by using the update interface, and records an available remittance path of the participant in the first smart contract. Certainly, the first smart contract can alternatively be created and deployed in a blockchain by a user of the blockchain.
15 For example, the first smart contract can be created by a participant of the target remittance transaction. In this way, in a process of creating the first smart contract, the participant of the target remittance transaction can directly deploy the available remittance path together with the first smart contract on the blockchain.

[0056] FIG. 3 is a schematic flowchart of a method for managing a remittance path based on a
20 blockchain according to an embodiment of the present disclosure. The method shown in FIG. 3 includes step S310 to step S330. The method shown in FIG. 3 can be applied to the blockchain architecture shown in FIG. 1. In this way, the first participant that performs step S310 may be a user 120 of the blockchain, for example, a user node 121 of a remittance bank or a user node 123 of a payee bank. Correspondingly, the blockchain node that performs steps S320 and S330 may be one
25 or more blockchain nodes 110 that can communicate with the user 120 in the architecture 100.

[0057] In step S310, the first participant obtains an available remittance path of the first participant.

[0058] The available remittance path of the first participant may be understood as an available remittance path of the first participant to be uploaded to the blockchain. For example, the available
30 remittance path may be an available remittance path of the first participant that needs to be updated. For another example, the available remittance path may be an available remittance path newly created by the first participant.

[0059] In step S320, the blockchain node receives a first invoking request of the first smart contract from the first participant.

[0060] The first participant is one participant among the plurality of participants involved in the target remittance transaction. The first participant may be a remittance bank that executes the target remittance transaction, and the first participant may alternatively be a payee bank that executes the target remittance transaction.

5 **[0061]** The first invoking request is used to set the available remittance path of the first participant. In some implementations, the above-mentioned setting may be understood as creating. In this case, the first invoking request may be understood as being used to create the available remittance path of the first participant. In some other implementations, the above-mentioned setting may be understood as updating. In this case, the first invoking request may be understood as being
10 used to update the available remittance path of the first participant.

[0062] In step S330, the blockchain node sets the available remittance path of the first participant in the first smart contract based on the first invoking request.

[0063] Generally, to improve security of the available remittance path, before step S330, the blockchain node can perform user authentication on the first participant, so as to determine that the
15 first participant has the right to set the available remittance path. For example, it is confirmed that the first participant is an on-chain user, and a role of the first participant is a bank. In this case, the first participant has the right to set the available remittance path. In some implementations, the user authentication can be implemented based on a public key and a data signature. Specifically, the blockchain node can store a public key of the first participant, and when the first participant sets the
20 available remittance path, the first participant can use a private key of the first participant to digitally sign the available remittance path. In this way, when the blockchain node receives the available remittance path uploaded by the first participant, the blockchain node can use the public key of the first participant to verify the digital signature on the available remittance path. If the verification succeeds, the first participant has the right to set the available remittance path. On the
25 contrary, if the verification fails, the first participant has no right to set the available remittance path.

[0064] In addition, to confirm validity of the available remittance path that is set by the first participant, before step S330, the blockchain node can further perform validity verification on the available remittance path uploaded by the first participant. In some implementations, the blockchain
30 can determine, based on a format of an available remittance path specified by the remittance path (which may be, for example, the format shown in Table 1), whether both a remittance party and a payee involved in the available remittance path are legal on-chain users. If both the remittance party and the payee are legal on-chain users, the blockchain node can determine that the available remittance path set by the first participant is legal, and the blockchain node can maintain the

available remittance path in the first smart contract. On the contrary, if the remittance party and/or the payee is not a legal on-chain user, the blockchain node can determine that the available remittance path set by the first participant is illegal, and the blockchain node does not maintain the available remittance path.

5 [0065] In some implementations, the blockchain node determines whether the remittance party and the payee involved in the available remittance path are legal on-chain users, and can perform the determining by determining whether the remittance party and the payee have corresponding on-chain users. For example, the blockchain node can store mapping relationships between on-chain user names of all on-chain users and off-chain user names of the users, and the remittance party and
10 the payee of the above-mentioned available remittance path use off-chain user names (for example, names of banks) of the remittance party and the payee. In this case, the blockchain can determine, based on the above-mentioned mapping relationships, and the off-chain user names of the remittance party and the payee, whether the remittance party and the payee have corresponding on-chain user names, so as to determine whether the remittance party and the payee are legal
15 on-chain users.

[0066] For ease of understanding of the present disclosure, the following uses updating the first smart contract as an example to describe a process of updating the first smart contract in an embodiment of the present disclosure with reference to FIG. 4. It should be noted that FIG. 4 mainly describes a method procedure for updating the first smart contract. For related descriptions
20 of content such as the first participant, the first smart contract, the available remittance path, the user authentication, and the validity verification, references can be made to the foregoing description. For brevity, details are not described herein again.

[0067] FIG. 4 is a schematic flowchart of a process of updating a first smart contract according to an embodiment of the present disclosure. The method shown in FIG. 4 includes step S410 to step
25 S460.

[0068] In step S410, a first participant sets a list of updated available remittance paths.

[0069] The first participant can input a first available remittance transfer list by invoking an update interface of the first smart contract.

[0070] In step S420, a blockchain node performs user authentication on the first participant.

30 [0071] The above-mentioned updated remittance paths are digitally signed by using a private key of the first participant. The blockchain node can verify the digital signature based on a public key of the first participant, so as to determine that user authentication is performed on the first participant. If the user authentication succeeds, step S430 can be performed. If the user authentication fails, the update fails. In this case, step S440 is performed to end the update process.

[0072] In step S430, the blockchain node performs validity verification on the available remittance paths in the list of available remittance paths.

[0073] If the validity verification succeeds, step S450 is performed. If the validity verification fails, the update fails. In this case, step S440 is performed.

5 [0074] In step S450, the blockchain node updates the available remittance path in the first smart contract into the above-mentioned first available remittance path list.

[0075] In step S460, the first smart contract is updated successfully.

[0076] The blockchain node can use the above-mentioned first available remittance path list as data of the first smart contract, and persistently store the first available remittance path list in the
10 blockchain.

[0077] It should be noted that an execution sequence of step S420 and step S430 is not limited in the present disclosure. Step S430 can alternatively be performed before step S420. In this case, step S420 can be performed when the validity verification in step S430 succeeds. In addition, step S450 can be performed only when the user authentication in step S420 succeeds. Certainly, step
15 S420 and step S430 can alternatively be performed at the same time, that is, step S450 can be performed only when the user authentication in step S420 succeeds and the validity verification in step S430 succeeds.

[0078] As described above, in the conventional process of initiating a remittance transaction, the remittance initiator needs to query the available remittance paths of the participants in the
20 centralized system first. However, in some cases, the remittance initiator may not query the available remittance path first based on the process, but directly initiates a first transaction execution request on the chain to request the first participant to execute the target remittance transaction. In this case, if the remittance path needed by the target remittance transaction does not match the available remittance path of the first participant, the first participant needs to confirm that
25 the available remittance path does not match the remittance path needed by the target remittance transaction, and then the first transaction initiated on the chain can be closed. However, if the first participant fails to perform timely confirmation, the transaction status of the first transaction remains stagnant and is in a state of "waiting for the first participant to confirm". In this case, the remittance initiator cannot learn a final execution result of the first transaction in a timely manner,
30 degrading user experience.

[0079] To avoid the above-mentioned problem, the present disclosure further provides a method for managing a remittance path based on a blockchain. Matching is performed between an available remittance path recorded in a first smart contract and a remittance path needed by a target remittance transaction, to obtain a matching result, and a transaction status of the first transaction is

automatically advanced based on the matching result. This avoids a case in which in a conventional manner of committing a remittance transaction, the transaction status of the first transaction remains stagnant because the first participant fails to perform timely confirmation, and consequently, the remittance initiator cannot learn a final execution result of the first transaction in a timely manner.

5 Therefore, the method for managing a remittance path based on a blockchain helps improve user experience.

[0080] Still referring to FIG. 3, the above-mentioned method may further include step S340 to step S360.

[0081] In step S340, a first transaction execution request is received from a second participant,
10 where the first transaction execution request is used to request the first participant to execute the target remittance transaction.

[0082] The second participant may be the initiator of the target remittance transaction, for example, may be the capitalist A described above.

[0083] In step S350, the first smart contract is invoked in response to the first transaction
15 execution request to query whether a remittance path needed by the target remittance transaction matches the available remittance path of the first participant.

[0084] If the remittance path needed by the target remittance transaction matches the available remittance path of the first participant, it may be understood that the available remittance path of the first participant includes the remittance path needed by the target remittance transaction. For
20 example, the remittance path needed by the target remittance transaction is remittance from bank A to bank B. In this case, if bank A serves as the first participant, and referring to Table 1, it can be learned that an available remittance path of bank A includes "bank A - bank B", the available remittance path of bank A matches the remittance path needed by the target remittance transaction.

[0085] If the remittance path needed by the target remittance transaction does not match the
25 available remittance path of the first participant, it may be understood that the available remittance path of the first participant does not include the remittance path needed by the target remittance transaction. For example, the remittance path needed by the target remittance transaction is remittance from bank A to bank C. In this case, if bank A serves as the first participant, and referring to Table 1, it can be learned that an available remittance path of the bank does not include a
30 remittance path of "bank A - bank C", the available remittance path of bank A does not match the remittance path needed by the target remittance transaction.

[0086] In step S360, if the remittance path needed by the target remittance transaction does not match the available remittance path of the first participant, the target remittance transaction is terminated.

[0087] The terminating the target remittance transaction may be understood as setting the transaction status of the first transaction to termination.

[0088] In some implementations, the above-mentioned solution described with reference to step S340 to step S360 can initiate a target remittance transaction to the blockchain by invoking a contract. In other words, the second participant can request the first participant to execute the target remittance transaction by invoking the contract. Alternatively, the first transaction execution request is a invoking request of a second smart contract, the second smart contract is used to execute the target remittance transaction, and a status of the second smart contract is used to indicate a transaction status of the target remittance transaction. Therefore, the second smart contract is also referred to as a "remittance transaction contract". The second smart contract may include transaction information of the target remittance transaction, for example, initiator information of the target remittance transaction, payee information of the target remittance transaction, the remittance path needed by the target remittance transaction, and transaction details of the target remittance transaction.

[0089] To associate the above-mentioned matching result with a status of the second smart contract, an address of the first smart contract can be set in the second smart contract. In this way, in a process of executing the second smart contract, the first smart contract can be invoked based on the address, so as to query whether the remittance path needed by the target remittance transaction matches the available remittance path of the first participant. If the remittance path needed by the target remittance transaction does not match the available remittance path of the first participant, the target remittance transaction can be terminated and the status of the second smart contract is set to closure. If the remittance path needed by the target remittance transaction matches the available remittance path of the first participant, the status of the second smart contract can be advanced to a next state (e.g., waiting for the participant to confirm the current transaction).

[0090] As described above, all participants on the blockchain can serve as users of the blockchain, and set respective available remittance paths by invoking the first smart contract. In other words, the first smart contract records available remittance paths of a plurality of participants. In this case, in some situations, a remittance path 1 may be an available remittance path for a participant 1, but the remittance path 1 is not an available remittance path for a participant 2. In this case, if matching is performed only on the available remittance path of the participant 1 in a matching process, a matching result becomes matched. However, the remittance path 1 is actually not an available remittance path, and the target remittance transaction fails.

[0091] It is assumed that the remittance path 1 is originally an available remittance path between bank A and bank B, but for some reasons, bank B and bank A need to update the available

remittance path, so as to update the remittance path 1 into an unavailable remittance path. However, only bank B succeeds in updating, and bank A fails to update. In this case, the remittance path 1 is no longer an available remittance path between bank A and bank B, but it is still recorded in the available remittance path of bank A. In this case, if the remittance path needed by the initiated target remittance transaction is just the available remittance path 1, and when only the available remittance path of bank A is used for matching, the matching result indicates matched, causing a failure of the target remittance transaction.

[0092] Therefore, to improve accuracy of the above-mentioned matching result, in a matching process, matching can be performed between the remittance path needed by the target remittance transaction and an available remittance path of each participant among a plurality of participants of the target remittance transaction. The remittance path is a real available remittance path only when all matching results indicate matched. Still referring to the above-mentioned scenario of the remittance path 1, in this case, matching is performed between the remittance path 1 and each of the available remittance path of bank A and the available remittance path of bank B. A result of the matching between the remittance path 1 and the available remittance path of bank A indicates matched, and a result of the matching between the remittance path 1 and the available remittance path of bank B indicates mismatched. Finally, the matching result corresponding to the remittance path 1 becomes mismatched, and the target remittance transaction can be directly terminated.

[0093] For ease of understanding of the present disclosure, the following describes a process of using the first smart contract in an embodiment of the present disclosure with reference to FIG. 5 by using an example in which the first smart contract is invoked in a process of executing the second smart contract. It should be noted that FIG. 5 mainly describes a method procedure for using the first smart contract. For related descriptions of content such as the first participant, the first smart contract, the available remittance path, the user authentication, and the validity verification, references can be made to the foregoing description. For brevity, details are not described herein again.

[0094] FIG. 5 is a schematic flowchart of a process of using a first smart contract according to an embodiment of the present disclosure. The method shown in FIG. 5 includes step S510 to step S590.

[0095] In step S510, a remittance initiator sends an invoking request of a second smart contract to a blockchain node.

[0096] The invoking request is used to request the first participant to execute the target remittance transaction. A remittance path needed by the target remittance transaction is a remittance path between the first participant and the second participant.

[0097] In step S520, the blockchain node performs user authentication on the remittance initiator.

[0098] The remittance initiator signs the invoking request of the second smart contract by using a private key. Correspondingly, after receiving the invoking request of the second smart contract, the blockchain node can verify the digital signature by using a public key of the remittance initiator. If a result of the user authentication indicates a success, step S530 is performed. If the result of the user authentication indicates a failure, step S540 is performed to close the target remittance transaction.

[0099] In step S530, the blockchain node performs validity verification on the second smart contract.

[0100] The above-mentioned validity verification is used to verify whether a transaction parameter of the target remittance transaction is complete. For example, the second smart contract needs to specify information such as on-chain accounts of the remittance institution and the payee institution of the target remittance transaction, and a remittance currency involved in the target remittance transaction.

[0101] If a result of the validity verification indicates a success, step S550 is performed. If the result of the validity verification indicates a failure, step S540 is performed to close the target remittance transaction.

[0102] In step S550, the remittance path needed by the target remittance transaction is extracted from the second smart contract.

[0103] In step S560, the blockchain node invokes the first smart contract to query whether the remittance path needed by the target remittance transaction separately matches the available remittance path of the remittance institution and the available remittance path of the payee institution.

[0104] In a process of executing the second smart contract, a query interface of the first smart contract can be automatically invoked twice to separately query whether the available remittance path of the remittance institution and the available remittance path of the payee institution match the remittance path needed by the target remittance transaction. If the available remittance path of the remittance institution and the available remittance path of the payee institution each match the remittance path needed by the target remittance transaction, step S570 is performed. If the available remittance path of the remittance institution and/or the available remittance path of the payee institution does not match the remittance path needed by the target remittance transaction, step S540 is performed to close the target remittance transaction.

[0105] In step S570, the blockchain node advances the status of the second smart contract to

"waiting for the participant to confirm the current transaction".

[0106] In step S580, the participant of the target remittance transaction confirms the target remittance transaction corresponding to the second smart contract.

[0107] The participant of the target remittance transaction can obtain transaction information of the target remittance transaction recorded in the second smart contract from the blockchain node through pull block parsing or the like. After confirming, based on the transaction information of the target remittance transaction, that the off-chain remittance transaction is correctly executed, the participant of the target remittance transaction can invoke a confirmation interface of the second smart contract to confirm the target remittance transaction.

[0108] In step S590, whether all participants of the target remittance transaction perform confirmation is confirmed.

[0109] After receiving the confirmation from the participant of the target remittance transaction, the second smart contract automatically triggers the processing logic to query whether all participants of the target remittance transaction have confirmed the target remittance transaction. If all participants of the target remittance transaction perform confirmation, the second smart contract automatically advances the status to a final state, indicating that the target remittance transaction is successful, that is, step S600.

[0110] It should be noted that an execution sequence of step S520 and step S530 is not limited in the present disclosure. Step S530 can alternatively be performed before step S520. In this case, step S520 can be performed when the validity verification in step S530 succeeds. In addition, step S550 can be performed only when the user authentication in step S520 succeeds. Certainly, step S520 and step S530 can alternatively be performed at the same time, that is, step S550 can be performed only when the user authentication in step S520 succeeds and the validity verification in step S530 succeeds.

[0111] The process of using the first smart contract in an embodiment of the present disclosure has been described above with reference to FIG. 5 by using an example in which the second smart contract invokes the first smart contract. In this embodiment of the present disclosure, an available remittance path can alternatively be queried only by using a query interface of the first smart contract. With reference to FIG. 6, the following describes a process of querying a first smart contract according to an embodiment of the present disclosure. It should be noted that FIG. 6 mainly describes a method procedure for using the first smart contract. For related descriptions of content such as the first participant, the first smart contract, and the available remittance path, references can be made to the foregoing description. For brevity, details are not described herein again.

[0112] FIG. 6 is a schematic flowchart of a process of querying a first smart contract according to an embodiment of the present disclosure. The method shown in FIG. 6 includes step S610 and step S620.

[0113] In step S610, a blockchain node receives a second invoking request of a first smart contract from a third participant, where the second invoking request is used to query an available remittance path of a first participant.

[0114] In step S620, the blockchain node returns the available remittance path of the first participant to the third participant.

[0115] Method embodiments of the present disclosure are described in detail above with reference to FIG. 1 to FIG. 6. Apparatus embodiments of the present disclosure are described in detail below with reference to FIG. 7 to FIG. 10. It should be understood that the descriptions of the method embodiments correspond to the descriptions of the apparatus embodiments. Therefore, for a part not described in detail, references can be made to the above-mentioned method embodiments.

[0116] FIG. 7 is a schematic structural diagram of an apparatus for managing a remittance path based on a blockchain according to an embodiment of the present disclosure. The apparatus shown in FIG. 7 may be a blockchain node on a blockchain, where the blockchain stores a first smart contract, the first smart contract is used to manage an available remittance path of at least one participant among a plurality of participants of a target remittance transaction, the available remittance path of the at least one participant is used to indicate an available remittance path that can be provided by the at least one participant for the target remittance transaction, and the at least one participant includes a first participant. The apparatus 700 includes a receiving module 710 and a processing module 720.

[0117] The receiving module 710 can be configured to receive a first invoking request of the first smart contract from the first participant, where the first invoking request is used to set an available remittance path of the first participant.

[0118] The processing module 720 can be configured to set the available remittance path of the first participant in the first smart contract based on the first invoking request.

[0119] Optionally, in some embodiments, the plurality of participants include a second participant; the receiving module 710 can be further configured to receive a first transaction execution request from the second participant, where the first transaction execution request is used to request the first participant to execute the target remittance transaction; the processing module 720 can be configured to invoke the first smart contract in response to the first transaction execution request to query whether a remittance path needed by the target remittance transaction matches the available remittance path of the first participant; and terminate the target remittance transaction if

the remittance path needed by the target remittance transaction does not match the available remittance path of the first participant.

[0120] Optionally, in some embodiments, the plurality of participants include a third participant; the receiving module 710 can be configured to receive a second invoking request of the first smart contract from the third participant, where the second invoking request is used to query the available remittance path of the first participant; the processing module 720 can be configured to return the available remittance path of the first participant to the third participant.

[0121] Optionally, in some embodiments, the receiving module 710 can be configured to receive a third invoking request of the first smart contract from the first participant, where the third invoking request is used to update the available remittance path of the first participant; the processing module 720 can be configured to update the available remittance path of the first participant in the first smart contract based on the third invoking request.

[0122] Optionally, in some embodiments, the first smart contract is further used to manage a currency type supported by the available remittance path of the first participant.

[0123] FIG. 8 is a schematic structural diagram of an apparatus for managing a remittance path based on a blockchain according to another embodiment of the present disclosure. The blockchain stores a first smart contract, the first smart contract is used to manage an available remittance path of at least one participant among a plurality of participants of a target remittance transaction, the available remittance path of the at least one participant is used to indicate an available remittance path that can be provided by the at least one participant for the target remittance transaction, the at least one participant includes a first participant, and the apparatus is applied to the first participant. The apparatus 800 includes an obtaining module 810 and a sending module 820.

[0124] The obtaining module 810 is configured to obtain an available remittance path of the first participant. The sending module 820 is configured to send a first invoking request of the first smart contract to the blockchain, where the first invoking request is used to set the available remittance path of the first participant.

[0125] Optionally, in some embodiments, the sending module 820 can be configured to send a third invoking request of the first smart contract to the blockchain, where the third invoking request is used to update the available remittance path of the first participant.

[0126] Optionally, in some embodiments, the first smart contract is further used to manage a currency type supported by the available remittance path of the first participant.

[0127] FIG. 9 is a schematic structural diagram of an apparatus for managing a remittance path based on a blockchain according to still another embodiment of the present disclosure. The apparatus 900 shown in FIG. 9 may be any blockchain node in the blockchain. The apparatus 900

may be, for example, a computing device with a computing function. For example, the apparatus 900 may be a server. The apparatus 900 may include a memory 910 and a processor 920. The memory 910 can be configured to store executable code. The processor 920 can be configured to execute the executable code stored in the memory 910 to implement the steps in the methods described above. In some embodiments, the apparatus 900 may further include a network interface 930, and data exchange between the processor 920 and an external device can be implemented by using the network interface 930.

[0128] FIG. 10 is a schematic structural diagram of an apparatus for managing a remittance path based on a blockchain according to still another embodiment of the present disclosure. The apparatus 1000 shown in FIG. 10 may be a node on which a client is located in the blockchain. The apparatus 1000 may be, for example, a computing device with a computing function. For example, the apparatus 1000 may be a server or a mobile terminal. The apparatus 1000 may include a memory 1010 and a processor 1020. The memory 1010 can be configured to store executable code. The processor 1020 can be configured to execute the executable code stored in the memory 1010 to implement the steps in the methods described above. In some embodiments, the apparatus 1000 may further include a network interface 1030, and data exchange between the processor 1020 and an external device can be implemented by using the network interface 1030.

[0129] It should be understood that, in the embodiments of the present disclosure, the processor may be a central processing unit (CPU), or may be another general-purpose processor, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a field programmable gate array (FPGA) or another programmable logic device, a discrete gate or a transistor logic device, a discrete hardware component, or the like. The general-purpose processor may be a microprocessor or the processor may be any conventional processor or the like, and is configured to execute a related program, to implement the technical solutions provided in the embodiments of the present disclosure.

[0130] The memory may include a read-only memory and a random access memory, and provide an instruction and data to the processor. A part of the processor may further include a non-volatile random access memory. For example, the processor may further store device type information.

[0131] In an implementation process, the steps of the above-mentioned methods can be completed by using an integrated logic circuit of hardware in the processor, or by using instructions in a form of software. The method for requesting an uplink transmission resource disclosed with reference to the embodiments of the present disclosure can be directly performed and completed by a hardware processor, or can be performed and completed by using a combination of hardware and

software modules in the processor. The software module can be located in a mature storage medium in the art, such as a random access memory, a flash memory, a read-only memory, a programmable read-only memory, an electrically erasable programmable memory, or a register. The storage medium is located in the memory, and the processor reads information in the memory and completes the steps of the above-mentioned methods in combination with hardware of the processor. To avoid repetition, details are not described herein again.

[0132] It should be understood that the term "and/or" in this specification means only an association relationship for describing associated objects and represents that three relationships may exist. For example, A and/or B may represent the following three cases: Only A exists, both A and B exist, and only B exists. In addition, the character "/" in this specification generally indicates an "or" relationship between associated objects.

[0133] It should be understood that sequence numbers of the above-mentioned processes do not mean execution sequences in the embodiments of the present disclosure. The execution sequences of the processes should be determined based on functions and internal logic of the processes, and should not be construed as any limitation on the implementation processes of the embodiments of the present disclosure.

[0134] In the several embodiments provided in the present disclosure, it should be understood that the disclosed system, apparatus, and method can be implemented in other ways. For example, the apparatus embodiments described above are merely examples. For example, the unit division is merely logical function division and may be other division in actual implementation. For example, a plurality of units or components can be combined or integrated into another system, or some features may be ignored or not performed. In addition, the displayed or discussed mutual couplings or direct couplings or communication connections can be implemented through some interfaces. The indirect couplings or communication connections between the apparatuses or units can be implemented in electronic, mechanical, or other forms.

[0135] The units described as separate components may or may not be physically separate, and components displayed as units may or may not be physical units, can be located in one position, or can be distributed on a plurality of network units. Some or all of the units can be selected depending on actual needs to achieve the purposes of the solutions of the embodiments.

[0136] In addition, functional modules in the embodiments of the present disclosure can be integrated into one module, or each of the modules can exist alone, or two or more modules can be integrated into one module.

[0137] All or some of the above-mentioned embodiments can be implemented by software, hardware, firmware, or any combination thereof. When being implemented by software, the

embodiments can be implemented completely or partially in a form of a computer program product. The computer program product includes one or more computer instructions. When the computer program instructions are loaded and executed on the computer, the procedure or functions according to the embodiments of the present disclosure are completely or partially generated. The computer
5 may be a general-purpose computer, a dedicated computer, a computer network, or another programmable apparatus. The computer instructions can be stored in a computer-readable storage medium or can be transmitted from a computer-readable storage medium to another computer-readable storage medium. For example, the computer instructions can be transmitted from a website, computer, server, or data center to another website, computer, server, or data center in a
10 wired (for example, a coaxial cable, an optical fiber, or a digital subscriber line (DSL)) or wireless (for example, infrared, radio, or microwave) manner. The computer-readable storage medium may be any usable medium accessible by a computer, or a data storage device, such as a server or a data center, integrating one or more usable media. The usable medium may be a magnetic medium (such as a floppy disk, a hard disk, or a magnetic tape), an optical medium (such as a digital versatile disc
15 (DVD), or a semiconductor medium (such as a solid state disk (SSD)), or the like.

[0138] The foregoing descriptions are merely specific implementations of the present disclosure, but are not intended to limit the protection scope of the present disclosure. Any variation or replacement readily figured out by a person skilled in the art within the technical scope disclosed in the present disclosure shall fall within the protection scope of the present disclosure. Therefore,
20 the protection scope of the present disclosure shall be subject to the protection scope of the claims.

CLAIMS

What is claimed is:

1. A method for managing a remittance path based on a blockchain, wherein the blockchain stores a first smart contract, the first smart contract is used to manage an available remittance path of at least one participant among a plurality of participants of a target remittance transaction, the available remittance path of the at least one participant is used to indicate an available remittance path that can be provided by the at least one participant for the target remittance transaction, and the at least one participant comprises a first participant;

the method comprises:

receiving a first invoking request of the first smart contract from the first participant, wherein the first invoking request is used to set an available remittance path of the first participant; and

setting the available remittance path of the first participant in the first smart contract based on the first invoking request.

2. The method according to claim 1, wherein the plurality of participants comprise a second participant, and the method further comprises:

receiving a first transaction execution request from the second participant, wherein the first transaction execution request is used to request the first participant to execute the target remittance transaction;

invoking the first smart contract in response to the first transaction execution request to query whether a remittance path needed by the target remittance transaction matches the available remittance path of the first participant; and

terminating the target remittance transaction if the remittance path needed by the target remittance transaction does not match the available remittance path of the first participant.

3. The method according to claim 1, wherein the plurality of participants comprise a third participant, and the method further comprises:

receiving a second invoking request of the first smart contract from the third participant, wherein the second invoking request is used to query the available remittance path of the first participant; and

returning the available remittance path of the first participant to the third participant.

4. The method according to claim 1, wherein the method further comprises:

receiving a third invoking request of the first smart contract from the first participant, wherein the third invoking request is used to update the available remittance path of the first participant; and

updating the available remittance path of the first participant in the first smart contract based on the third invoking request.

5. The method according to any one of claims 1 to 4, wherein the first smart contract is further used to manage a currency type supported by the available remittance path of the first participant.

6. A method for managing a remittance path based on a blockchain, wherein the blockchain stores a first smart contract, the first smart contract is used to manage an available remittance path of at least one participant among a plurality of participants of a target remittance transaction, the available remittance path of the at least one participant is used to indicate an available remittance path that can be provided by the at least one participant for the target remittance transaction, the at least one participant comprises a first participant, and the method is applied to the first participant;

the method comprises:

obtaining an available remittance path of the first participant; and

sending a first invoking request of the first smart contract to the blockchain, wherein the first invoking request is used to set the available remittance path of the first participant.

7. The method according to claim 6, wherein the method further comprises:

sending a third invoking request of the first smart contract to the blockchain, wherein the third invoking request is used to update the available remittance path of the first participant.

8. The method according to claim 6 or 7, wherein the first smart contract is further used to manage a currency type supported by the available remittance path of the first participant.

9. An apparatus for managing a remittance path based on a blockchain, wherein the blockchain stores a first smart contract, the first smart contract is used to manage an available remittance path of at least one participant among a plurality of participants of a target remittance transaction, the available remittance path of the at least one participant is used to indicate an available remittance path that can be provided by the at least one participant for the target remittance transaction, and the at least one participant comprises a first participant;

the apparatus comprises:

a receiving module, configured to receive a first invoking request of the first smart contract from the first participant, wherein the first invoking request is used to set an available remittance path of the first participant; and

a processing module, configured to set the available remittance path of the first participant in the first smart contract based on the first invoking request.

10. The apparatus according to claim 9, wherein the plurality of participants comprise a second participant;

the receiving module is configured to receive a first transaction execution request from the second participant, wherein the first transaction execution request is used to request the first participant to execute the target remittance transaction;

the processing module is configured to invoke the first smart contract in response to the first transaction execution request to query whether a remittance path needed by the target remittance transaction matches the available remittance path of the first participant; and

the processing module is configured to terminate the target remittance transaction if the
5 remittance path needed by the target remittance transaction does not match the available remittance path of the first participant.

11. The apparatus according to claim 9, wherein the plurality of participants comprise a third participant;

the receiving module is configured to receive a second invoking request of the first smart
10 contract from the third participant, wherein the second invoking request is used to query the available remittance path of the first participant; and

the processing module is configured to return the available remittance path of the first participant to the third participant.

12. The apparatus according to claim 9, wherein

15 the receiving module is configured to receive a third invoking request of the first smart contract from the first participant, wherein the third invoking request is used to update the available remittance path of the first participant; and

the processing module is configured to update the available remittance path of the first participant in the first smart contract based on the third invoking request.

20 13. The apparatus according to any one of claims 9 to 12, wherein the first smart contract is further used to manage a currency type supported by the available remittance path of the first participant.

14. An apparatus for managing a remittance path based on a blockchain, wherein the blockchain stores a first smart contract, the first smart contract is used to manage an available
25 remittance path of at least one participant among a plurality of participants of a target remittance transaction, the available remittance path of the at least one participant is used to indicate an available remittance path that can be provided by the at least one participant for the target remittance transaction, the at least one participant comprises a first participant, and the apparatus is applied to the first participant;

30 the apparatus comprises:

an obtaining module, configured to obtain an available remittance path of the first participant;
and

a sending module, configured to send a first invoking request of the first smart contract to the blockchain, wherein the first invoking request is used to set the available remittance path of the first

participant.

15. The apparatus according to claim 14, wherein

the sending module is configured to send a third invoking request of the first smart contract to the blockchain, wherein the third invoking request is used to update the available remittance path of the first participant.

16. The apparatus according to claim 14 or 15, wherein the first smart contract is further used to manage a currency type supported by the available remittance path of the first participant.

17. An apparatus for managing a remittance path based on a blockchain, comprising a memory and a processor, wherein the memory stores executable code, and the processor is configured to execute the executable code to implement the method according to any one of claims 1 to 5.

18. An apparatus for managing a remittance path based on a blockchain, comprising a memory and a processor, wherein the memory stores executable code, and the processor is configured to execute the executable code to implement the method according to any one of claims 6 to 8.