REGULATING BLOCKCHAIN CONFIDENTIAL TRANSACTIONS

BACKGROUND

[0001] Distributed ledger systems (DLSs), which can also be referred to as consensus networks, and/or blockchain networks, enable participating entities to securely, and immutably store data. DLSs are commonly referred to as blockchain networks without referencing any particular user case (e.g., crypto-currencies). Example types of blockchain networks can include public blockchain networks, private blockchain networks, and consortium blockchain networks. A public blockchain network is open for all entities to use the DLS, and participate in the consensus process. A private blockchain network is provided for particular entity, which centrally controls read and write permissions. A consortium blockchain network is provided for a select group of entities, which control the consensus process, and includes an access control layer.

[0002] Blockchains are used in crypto-currency networks, which enable participants to conduct transactions to buy/sell goods, and/or services using a crypto-currency. A common crypto-currency includes Bitcoin. In crypto-currency networks, record-keeping models are used to record transactions between users. Example record-keeping models include an unspent transaction output (UTXO) model, and account model (also referred to as account-based model or account/balance model).

[0003] In the UTXO model, the assets on the chain are in the form of transactions. Each transaction spends output from prior transactions and generates new outputs that can be spent in subsequent transactions. A user's unspent transactions are tracked, and a balance that the user has to spend is calculated as the sum of the unspent transactions. Each transaction takes one or more unspent outputs (and only unspent outputs) as input and can have one or more outputs. The requirement that only unspent outputs may be used in further transactions is necessary to prevent double spending and fraud. The UTXO model supports the transaction validation and proof function, but the support for smart contracts is weak.

[0004] The account model is adopted by Ethereum. The account model performs record-keeping and manages account balances like a traditional bank. Under this model, an account can have an address and a corresponding account balance. Assets on the chain are represented as the balance of the account. Each transfer transaction can have an account address of a transferred asset and an account address of a received asset. The transaction

amount is directly updated on the balance of the account. The account model is efficient as each transaction may only need to validate that the sending account has enough balance to pay for the transaction. In addition to supporting the transaction validation and proof function, the account model can fully support smart contracts, especially those that require state information or involve multiple parties.

SUMMARY

[0005] Implementations of the present disclosure include computer-implemented methods for confidential transactions based on blockchain technologies (referred to as blockchain confidential transactions or, simply, confidential transactions). More particularly, implementations of the present disclosure are directed to regulating blockchain confidential transactions.

[0006] In some implementations, actions include obtaining, by a client node of a blockchain network, a public key of a regulator node; generating, by the client node, one or more commitment values of a confidential transaction of the client node by applying a cryptographic commitment scheme to transaction data of the confidential transaction; generating, by the client node, encrypted regulatory information of the confidential transaction by encrypting the transaction data using the public key of the regulator node; and transmitting, by the client node to a consensus node of the blockchain network, a content of the confidential transaction for execution, wherein the content of the confidential transaction includes: the one or more commitment values; the encrypted regulatory information; and one or more zero-knowledge proofs of the transaction data. Other implementations include corresponding systems, apparatus, and computer programs, configured to perform the actions of the methods, encoded on computer storage devices.

[0007] In some implementations, actions include generating, by a regulator node of a blockchain network, a pair of a public key and a private key; publishing, by the regulator node, the public key to a plurality of client nodes of the blockchain network; obtaining, by the regulator node from a consensus node of the blockchain network, a content of a confidential transaction of a client node, wherein the content of the confidential transaction includes: one or more commitment values of the confidential transaction generated by the client node by applying a cryptographic commitment scheme to transaction data of the confidential transaction; one or more zero-knowledge proofs of the

transaction data; and encrypted regulatory information generated by the client node by encrypting the transaction data using the public key of the regulator node; obtaining the transaction data by decrypting the encrypted regulatory information using the private key of the regulator node; and verifying, by the regulator node, that the confidential transaction is legitimate based on the content of the confidential transaction and the decrypted transaction data.

[0008] These and other implementations may each optionally include one or more of the following features.

[0009] A first feature, combinable with any of the following features, wherein the transaction data of the confidential transaction includes one or both of an account balance of the client node before the confidential transaction or a transaction amount of the confidential transaction.

[0010] A second feature, combinable with any of the previous or following features, wherein the one or more zero-knowledge proofs of the transaction data includes one or more zero-knowledge range proofs that values of the transaction data are within respective ranges.

[0011] A third feature, combinable with any of the previous or following features, wherein the one or more zero-knowledge proofs of the transaction data includes a zero-knowledge proof that the client node uses the public key of the regulator node in generating the encrypted regulatory information of the confidential transaction.

[0012] A fourth feature, combinable with any of the previous or following features, wherein the cryptographic commitment scheme includes a Pedersen Commitment scheme; wherein generating one or more commitment values of a confidential transaction of the client node by applying a cryptographic commitment scheme to transaction data includes generating the one or more commitment values of the confidential transaction of the client node based on the transaction data and random numbers corresponding to the transaction data; and wherein generating encrypted regulatory information of the confidential transaction includes generating encrypted regulatory information of the confidential transaction by encrypting the transaction data and random numbers corresponding to the transaction data using the public key of the regulator node.

[0013] A fifth feature, combinable with any of the previous or following features, wherein the content of the confidential transaction further includes a digital signature of the client node.

[0014] A sixth feature, combinable with any of the previous or following features, wherein verifying that the confidential transaction is valid based on the content of the confidential transaction and the decrypted transaction data includes one or more of: determining that the one or more commitment values are correct based on the commitment scheme; verifying the one or more zero-knowledge proofs of the transaction data; or determining that values of the transaction data comply with regulation.

[0015] A seventh feature, combinable with any of the previous or following features, wherein verifying the one or more zero-knowledge proofs of the transaction data includes one or more of: determining that an account balance of the client node before the confidential transaction is larger than zero; determining that a transaction amount of the confidential transaction is larger than zero; and determining that a transaction amount of the confidential transaction is less than or equal to an account balance of the client node before the confidential transaction.

[0016] The present disclosure also provides one or more non-transitory computer-readable storage media coupled to one or more processors and having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations in accordance with implementations of the methods provided herein.

[0017] The present disclosure further provides a system for implementing the methods provided herein. The system includes one or more processors, and a computer-readable storage medium coupled to the one or more processors having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations in accordance with implementations of the methods provided herein.

[0018] It is appreciated that methods in accordance with the present disclosure may include any combination of the aspects and features described herein. That is, methods in accordance with the present disclosure are not limited to the combinations of

aspects and features specifically described herein, but also include any combination of the aspects and features provided.

[0019] The details of one or more implementations of the present disclosure are set forth in the accompanying drawings and the description below. Other features and advantages of the present disclosure will be apparent from the description and drawings, and from the claims.

DESCRIPTION OF DRAWINGS

[0020] FIG. 1 depicts an example environment that can be used to execute implementations of the present disclosure.

[0021] FIG. 2 depicts an example conceptual architecture in accordance with implementations of the present disclosure.

[0022] FIG. 3 depicts an example regulation process of a blockchain confidential transaction in accordance with implementations of the present disclosure.

[0023] FIG. 4 depicts an example content of a blockchain confidential transaction in accordance with implementations of the present disclosure.

[0024] FIG. 5 depicts an example process that can be executed in accordance with implementations of the present disclosure.

[0025] Like reference symbols in the various drawings indicate like elements.

DETAILED DESCRIPTION

[0026] Implementations of the present disclosure include computer-implemented methods for confidential transactions based on blockchain technologies (referred to as blockchain confidential transactions or, simply, confidential transactions). More particularly, implementations of the present disclosure are directed to regulating blockchain confidential transactions.

[0027] In some implementations, actions include obtaining, by a client node of a blockchain network, a public key of a regulator node; generating, by the client node, one or more commitment values of a confidential transaction of the client node by applying a cryptographic commitment scheme to transaction data of the confidential transaction; generating, by the client node, encrypted regulatory information of the confidential transaction by encrypting the transaction data using the public key of the regulator node; and transmitting, by the client node to a consensus node of the blockchain network, a

content of the confidential transaction for execution, wherein the content of the confidential transaction includes: the one or more commitment values; the encrypted regulatory information; and one or more zero-knowledge proofs of the transaction data.

[0028] In some implementations, actions include generating, by a regulator node of a blockchain network, a pair of a public key and a private key; publishing, by the regulator node, the public key to a plurality of client nodes of the blockchain network; obtaining, by the regulator node from a consensus node of the blockchain network, a content of a confidential transaction of a client node, wherein the content of the confidential transaction includes: one or more commitment values of the confidential transaction generated by the client node by applying a cryptographic commitment scheme to transaction data of the confidential transaction; one or more zero-knowledge proofs of the transaction data; and encrypted regulatory information generated by the client node by encrypting the transaction data using the public key of the regulator node; obtaining the transaction data by decrypting the encrypted regulatory information using the private key of the regulator node; and verifying, by the regulator node, that the confidential transaction is legitimate based on the content of the confidential transaction and the decrypted transaction data.

[0029] Other implementations include corresponding systems, apparatus, and computer programs, configured to perform the actions of the methods, encoded on computer storage devices. .

[0030] To provide further context for implementations of the present disclosure, and as introduced above, distributed ledger systems (DLSs), which can also be referred to as consensus networks (e.g., made up of peer-to-peer nodes), and blockchain networks, enable participating entities to securely, and immutably conduct transactions, and store data. Although the term blockchain is generally associated with the Bitcoin crypto-currency network, blockchain is used herein to generally refer to a DLS without reference to any particular use case. As introduced above, a blockchain network can be provided as a public blockchain network, a private blockchain network, or a consortium blockchain network.

[0031] In a public blockchain network, the consensus process is controlled by nodes of the consensus network. For example, hundreds, thousands, even millions of

entities can cooperate a public blockchain network, each of which operates at least one node in the public blockchain network. Accordingly, the public blockchain network can be considered a public network with respect to the participating entities. In some examples, a majority of entities (nodes) must sign every block in order for the block to be valid, and added to the blockchain (distributed ledger) of the blockchain network. An example public blockchain network includes the Bitcoin network, which is a peer-to-peer payment network. The Bitcoin network leverages a distributed ledger, referred to as blockchain. As noted above, the term blockchain, however, is used to generally refer to distributed ledgers without particular reference to the Bitcoin network.

[0032] In general, a public blockchain network supports public transactions. A public transaction is shared with all of the nodes within the public blockchain network, and are stored in a global blockchain. A global blockchain is a blockchain that is replicated across all nodes. That is, all nodes are in perfect state consensus with respect to the global blockchain. To achieve consensus (e.g., agreement to the addition of a block to a blockchain), a consensus protocol is implemented within the public blockchain network. An example consensus protocol includes, without limitation, proof-of-work (POW) implemented in the Bitcoin network.

[0033] In general, a private blockchain network is provided for a particular entity, which centrally controls read and write permissions. The entity controls, which nodes are able to participate in the blockchain network. Consequently, private blockchain networks are generally referred to as permissioned networks that place restrictions on who is allowed to participate in the network, and on their level of participation (e.g., only in certain transactions). Various types of access control mechanisms can be used (e.g., existing participants vote on adding new entities, a regulatory authority can control admission).

[0034] In general, a consortium blockchain network is private among the participating entities. In a consortium blockchain network, the consensus process is controlled by an authorized set of nodes, one or more nodes being operated by a respective entity (e.g., a financial institution, insurance company). For example, a consortium of ten (10) entities (e.g., financial institutions, insurance companies) can operate a consortium blockchain network, each of which operates at least one node in the consortium blockchain network. Accordingly, the consortium blockchain network can be considered a private

network with respect to the participating entities. In some examples, each entity (node) must sign every block in order for the block to be valid, and added to the blockchain. In some examples, at least a sub-set of entities (nodes) (e.g., at least 7 entities) must sign every block in order for the block to be valid, and added to the blockchain.

[0035] Implementations of the present disclosure are described in further detail herein with reference to a consortium blockchain network. It is contemplated, however, that implementations of the present disclosure can be realized in any appropriate type of blockchain network.

[0036] Implementations of the present disclosure are described in further detail herein in view of the above context. More particularly, and as introduced above, implementations of the present disclosure are directed to regulating blockchain confidential transactions.

[0037] A blockchain is a tamper-proof, shared digital ledger that records transactions in a public or private peer-to-peer network. The ledger is distributed to all member nodes in the network, and the history of asset transactions occurring in the network is permanently recorded in the block. Since the ledger is entirely public to the participating entities, the blockchain ledger itself has no privacy protection function and requires additional technology to protect the privacy of the content of asset transaction.

[0038] Techniques for privacy protection for blockchain can include those for realizing a confidential transaction to protect privacy of a content of a transaction. In a confidential transaction, the content of a transaction is only accessible or known by participants of the transaction, not any other outsiders. For example, a confidential transaction allows only the two parties partaking in the transaction to be privy to the amount being transacted, and outside observers are prevented from knowing this information. Such techniques for realizing confidential transactions have been used, for example, in MONERO and ZCASH.

[0039] Techniques for privacy protection for blockchain can also include those for protecting identities of parties to a transaction can be realize, for example, using a stealth address or a ring signature mechanism.

[0040] With privacy protection added to the blockchain (for example, in the context of confidential transactions), it is difficult for one or more regulators (such as

government, industry associations, etc.) to audit, exam, inspect, supervise, or otherwise regulate the transactions. For example, it is difficult for a regulator (or supervisor) in a consortium blockchain network to check formality and validity of the content of confidential transaction because the information of the transaction stored on the blockchain is encrypted, which would limit the applications of the blockchain.

[0041] Example techniques are described to solve the problem to make it possible and easier for the regulator to regulate the content on the blockchain, especially in the case of blockchain confidential transactions. The example techniques can be based on the account model and have the advantages of supporting smart contracts.

[0042] For example, when submitting a confidential transaction, a user can encrypt both a random number and a plaintext value (e.g., an account balance before the confidential transaction or a transfer amount of the confidential transaction) corresponding to the Pedersen Commitment in the transaction (described in greater detail below), and can use a public key of the regulator to encrypt and submit it as part of the transaction data. The regulator can use its private key to decrypt the Pedersen Commitment for each transaction at any time, thus determining whether each transaction meets regulatory requirements without any additional chain interactions such as sending a query to each participant in the chain at the time of the audit, receiving returned results from each participant to analyze the returned result to verify each transaction.

[0043] The proposed techniques can preserve the de-centralized property of the blockchain and do not require a central node or a third party, for example, that is relied on in a group signature-based technology or other techniques in implementing a regulatory solution in privacy protection of blockchain transactions. The proposed techniques do not require the regulator to sign each transaction before each transaction is submitted. Accordingly, the proposed techniques do not rely on a central node and thus avoid the central node in the blockchain network becoming a bottleneck in system performance, security, etc.

[0044] FIG. 1 depicts an example environment 100 that can be used to execute implementations of the present disclosure. In some examples, the example environment 100 enables entities to participate in a consortium blockchain network 102. The example environment 100 includes computing devices or systems 106, 108, and a network 110. In

some examples, the network 110 includes a local area network (LAN), wide area network (WAN), the Internet, or a combination thereof, and connects web sites, user devices (e.g., computing devices), and back-end systems. In some examples, the network 110 can be accessed over a wired and/or a wireless communications link.

[0045] In the depicted example, the computing systems 106, 108 can each include any appropriate computing system that enables participation as a node in the consortium blockchain network 102. Example computing devices include, without limitation, a server, a desktop computer, a laptop computer, a tablet computing device, and a smartphone. In some examples, the computing systems 106, 108 hosts one or more computer-implemented services for interacting with the consortium blockchain network 102. For example, the computing system 106 can host computer-implemented services of a first entity (e.g., user A), such as transaction management system that the first entity uses to manage its transactions with one or more other entities (e.g., other users). The computing system 108 can host computer-implemented services of a second entity (e.g., user B), such as transaction management system that the second entity uses to manage its transactions with one or more other entities (e.g., other users). In the example of FIG. 1, the consortium blockchain network 102 is represented as a peer-to-peer network of nodes, and the computing systems 106, 108 provide nodes of the first entity, and second entity respectively, which participate in the consortium blockchain network 102.

[0046] FIG. 2 depicts an example conceptual architecture 200 in accordance with implementations of the present disclosure. The example conceptual architecture 200 includes an entity layer 202, a hosted services layer 204, and a blockchain network layer 206. In the depicted example, the entity layer 202 includes three entities, Entity_1 (E1), Entity_2 (E2), and Entity_3 (E3), each entity having a respective transaction management system 208.

[0047] In the depicted example, the hosted services layer 204 includes interfaces 210 for each transaction management system 208. In some examples, a respective transaction management system 208 communicates with a respective interface 210 over a network (e.g., the network 110 of FIG. 1) using a protocol (e.g., hypertext transfer protocol secure (HTTPS)). In some examples, each interface 210 provides communication connection between a respective transaction management system 208, and the blockchain

network layer 206. More particularly, the interface 210 communicate with a blockchain network 212 of the blockchain network layer 206. In some examples, communication between an interface 210, and the blockchain network layer 206 is conducted using remote procedure calls (RPCs). In some examples, the interfaces 210 "host" blockchain network nodes for the respective transaction management systems 208. For example, the interfaces 210 provide the application programming interface (API) for access to blockchain network 212.

[0048] As described herein, the blockchain network 212 is provided as a peer-to-peer network including a plurality of nodes 214 that immutably record information in a blockchain 216. Although a single blockchain 216 is schematically depicted, multiple copies of the blockchain 216 are provided, and are maintained across the blockchain network 212. For example, each node 214 stores a copy of the blockchain. In some implementations, the blockchain 216 stores information associated with transactions that are performed between two or more entities participating in the consortium blockchain network.

[0049] FIG. 3 depicts an example regulation process 300 of a blockchain confidential transaction (transaction) in accordance with implementations of the present disclosure. A 302 and B 304 represent two client nodes of two users (also referred to as clients, entities, participants or parities) of a transaction and S 306 is a regulator (or supervisor) node in a blockchain network 350. The blockchain network 350 can include multiple consensus nodes (denoted as blockchain nodes 308 in FIG. 3).

[0050] In some implementations, A 302 and B 304 are examples of the computing systems 106, 108 corresponding to a first and second user or entity as described in FIGS. 1 and 2. Each client node A 302 or B 304 has a corresponding account (e.g., a public account or a private account) for transactions over the blockchain network 350.

[0051] In some implementations, client node A 302 can perform a confidential transaction with client node B 304 such that the transaction information is only viewable or otherwise known by client node A 302 and client node B 304, but not other parties (e.g., blockchain nodes 308) in the blockchain network 350.

[0052] In some implementations, some or all transactions performed in the blockchain network 350 may be subject to regulation by the regulator node S 306. For

example, the regulator node S 306 can determine whether a particular transaction complies with certain rules or regulations by, for example, monitoring, inspecting, auditing, supervising, or otherwise regulating the transaction. In some implementations, transaction information of a confidential transaction may be made available and viewable by the regulator node S 306.

[0053] In some implementations, to have access to transaction information of a confidential transaction while keeping the privacy of the confidential transaction, the regulator node S 306 can generate a pair of keys, a public key Spub 316 and a private key Spriv 326. The regulator node S 306 can publish or issues the public key Spub 316 to client nodes (e.g., A 302 and B 304) in the blockchain network 350 so that a client node can use the public key Spub 316 to encrypt the transaction information. Because it is encrypted, the transaction information is not viewable by other third-parties but accessible to the regulator node S 306 because the regulator node S 306 can decrypt the encrypted transaction information using its private key Spriv 326.

[0054] For example, as shown in FIG. 3, before the transaction, client node A 302 has an account balance a and client node B 304 has an account balance b. At 310, client node A 302 creates a confidential transaction to transfer an amount t to client node B 304. In some implementations, client node A 302 can construct a content of the confidential transaction locally and submit the content of the confidential transaction to the blockchain network 350 (e.g., one or more blockchain node 308 in the blockchain network 350).

[0055] FIG. 4 depicts an example content 400 of an example confidential transaction 450 in accordance with implementations of the present disclosure. As illustrated, the example confidential transaction 450 is the transfer of a transaction amount t from client node A 302 to client node B 304 as described with respect to FIG. 3.

[0056] In some implementations, the confidential transaction 450 can be constructed based on a commitment scheme to conceal the transaction data (e.g., the account balance before the transaction and the transaction amount). An example commitment scheme includes, without limitation, the Pedersen Commitment (PC). For example, the client node A 302 generates a commitment value based on a transaction amount t and a random number r using the PC. For example, the commitment value

includes a cypher text that can be obtained according to $PC(t) = rG + tH$, where G and H can be generators of an elliptical curve, $PC(t)$ is a scalar multiplication of curve points, t is the value that is committed to. The PC commitment scheme has a homomorphism, that is, $PC(t_1) + PC(t_2) = PC(t_1+t_2)$. Holders of the cypher text $PC(t)$ can verify the transaction amount t by using the random number r. Although implementations of the present disclosure are described in further detail herein with reference to the PC, it is contemplated that implementations of the present disclosure can be realized using any appropriate commitment scheme.

[0057] In the example confidential transaction 450, client node A 302 can commit to a pre-transaction account balance a and a transfer amount t. In some implementations, client node A 302 can generate a commitment value $PC(a)$ using PC based on the pre-transaction account balance a and a corresponding random number ra. Similarly, client node A 302 can generate a commitment value $PC(t)$ using PC based on the pre-transaction account balance a and a corresponding random number rt. In some implementations, client node A 302 can also commit that it has sufficient fund so that the post-transaction balance a-t is large than or equal to 0. For example, client node A 302 can generate a commitment value $PC(a\text{-}t)$, for example, based on the commitment values $PC(a)$ and $PC(t)$ given the homomorphic property of the PC. The commitment values can be included in the content 400 of the example confidential transaction 450.

[0058] In some implementations, additional or different commitment values can be included. For example, client node A 302 can commit that it uses the public key of the regulator (e.g., the public key Spub 316) to encrypt the transaction information. For example, client node A 302 can generate a commitment value $PC(Spub)$ based on Spub and the transaction information.

[0059] To facilitate the regulator's regulation, client node A 302 also can encrypt the transaction information, such as, amount a, t and corresponding random number ra, rt of each Pedersen Commitment involved in the transaction using the public key Spub of the regulator. For example, client node A 302 also can encrypt the transaction information (e.g., ra, a, rt, t) using the Spub and obtain encrypted regulatory information, e.g., a cipher text M denoted as encrypt (Spub, (ra|a|rt|t)). As an example, the cipher text M can be a concatenation of encrypted text of the four elements ra, a, rt, t, or in another format. In

some implementations, the encrypted regulatory information can include additional or different transaction information and may be generated in another manner.

[0060] In some implementations, the content 400 of the example confidential transaction 450 can include one or more zero knowledge proofs to enable a receiving party to confirm that the information the sending party is sending is valid. The zero knowledge proofs enable the receiving party to do this without actual knowledge of the information being confirmed. The zero knowledge proofs can include range proof such as Proof (a-t>0), Proof (t>0), and Proof (a>0), or other types of proofs. The zero knowledge proofs enable the receiving party (e.g., client node B) to confirm that the sending party (e.g., client node A) has enough funds to transfer (i.e., a-t>0), and that the transfer amount is greater than zero, without knowing either the balance *a* from which the amount is being transferred, or even the transfer amount *t*.

[0061] In some implementations, the content 400 of the example confidential transaction 450 can include other transaction-related information, such as A's digital signature on the transaction.

[0062] Referring back to FIG. 3, after generating the transaction content (e.g., the content 400 of the example confidential transaction), client node A 302 can submit the content of the confidential transaction to the blockchain network 350 (e.g., one or more blockchain node 308 in the blockchain network 350). At 320, the blockchain network 350 can execute the confidential transaction. In some implementations, the confidential transaction can be executed by each of the blockchain node 308 in the blockchain network 350. For example, each of the blockchain node 308 can determine whether the content of the confidential transaction is legitimate, for example, by verifying one or more commitment values and zero knowledge proofs included in the content of the confidential transaction. For example, each of the blockchain node 308 can verify the commitment values by verifying PC(a) = PC(t) + PC(a-t), that is, input transaction values is equal to output transaction values. Each of the blockchain node 308 can verify the zero knowledge proofs, for example, based on Bulletproofs, Monero's RingCT algorithms, or any other suitable algorithms.

[0063] Once the commitment values and zero knowledge proofs have been verified, each of the blockchain nodes 308 can record the transaction and update the

accounts of client node A 302 and client node B 304. For example, after the transaction, client node A 302 has an account balance a-t and client node B 304 has an account balance b+t. In some implementations, the post-transaction balance of client node A 302 and client node B 304 can be reflected by the direct operations of the commitment value due to the homomorphism of the commitment scheme. For example, client node A 302 can now have a commitment value of a post-transaction account balance PC (a-t) = PC(a) – PC(t). Client node B 304 can now have a commitment value of a post-transaction account balance PC(b+t) = PC(b) + PC(t).

[0064] At 330, to regulate the confidential transaction, the regulator node S 306 obtains the content of the confidential transaction from the blockchain network 350 and determine whether transaction information meets regulatory criteria or requirements. For example, the regulator node 306 can obtain the content of the confidential transaction that contains encrypted regulatory information (e.g., a cipher text M = encrypt (Spub, (ra|a|rt|t) as shown in FIG. 4). The regulator node S 306 uses its private key Spriv 326 to decrypt the encrypted regulatory information and obtains the plaintext transaction information (e.g., *ra, a, rt, t*) corresponding to the PCs in the transaction. The regulator node S 306 can determine whether transaction information meets regulatory criteria or requirements, verify the validity of the commitment values based on the plaintext transaction information. For example, the regulator node S 306 can perform traditional regulation such as determining whether the transaction amount is below a maximum permitted transaction amount.

[0065] In some implementations, the regulator node S 306 can subscribe to some or all transactions performed in the blockchain network 350 so that transaction data of the transactions can be pushed to the regulator node S 306 automatically. In some implementations, the regulator node S 306 can fetch, pull, or obtain transaction data of the some or all transaction from the blockchain network 350 (e.g., from one or more blockchain node 308 in the blockchain network 350).

[0066] FIG. 5 depicts an example process 500 that can be executed in accordance with implementations of the present disclosure. In some implementations, the example process 500 may be performed using one or more computer-executable programs executed using one or more computing devices. For clarity of presentation, the description that follows generally describes method 500 in the context of the other figures in this

description. For example, the regulator node 510 can be the regulator node S 306, the blockchain node 520 can be the blockchain node 308, client node A 530 can be client node A 302, and client node B 540 can be client node B 304 as described with respect to FIG. 3. However, it will be understood that method 500 may be performed, for example, by any suitable system, environment, software, and hardware, or a combination of systems, environments, software, and hardware, as appropriate. In some implementations, various steps of method 500 can be run in parallel, in combination, in loops, or in any order.

[0067] At 512, the regulator node 510 of a blockchain network generates a pair of a public key and a private key. The pair of the public key and the private key can be used for encrypting and decrypting transaction information for regulation.

[0068] At 514, the regulator node 510 publishes the public key to a plurality of client nodes (e.g., client node A 530 and client node B 540) of the blockchain network. For example, the regulator node 510 can issue the public key to all client nodes in the blockchain network (e.g., a consortium blockchain network) that are subject to the regulator node's regulation.

[0069] At 532, client node A 530, a client node of the blockchain network, obtains the public key of the regulator node 510. The client node A 530 can use the public key of the regulator node 510 to encrypt transaction data subject to regulation, thereby allowing the regulator node 510 to decrypt the transaction data using the private key corresponding to the public key.

[0070] The client node A 530 can prepare for a confidential transaction 535, such as a transfer of an amount of fund from an account of the client node A 530 to an account of client node B 540, another client node of the blockchain network. The client node A 530 can construct the content of the confidential transaction to protect privacy of transaction data and conceal the transaction data from inspection by other entities except the participants of the transaction (i.e., client node A 530 and client node B 540 in this example) and the regulator node 510. In some implementations, the client node A 530 can conceal the transaction data of the confidential transaction based on a commitment scheme.

[0071] In some implementations, the transaction data of the confidential transaction includes one or both of an account balance of the client node A 530 before the confidential transaction or a transaction amount of the confidential transaction. In some

implementations, the transaction data of the confidential transaction can include additional transaction information (e.g., time of the transaction, parties of the transaction, asset type (e.g., stock security or another type)).

[0072] At 534, the client node A 530 generates one or more commitment values of the confidential transaction of the client node A 530 by applying a cryptographic commitment scheme to transaction data of the confidential transaction. In some implementations, the cryptographic commitment scheme includes a homomorphic cryptographic commitment scheme, such as, a Pedersen Commitment scheme, or another type of commitment scheme.

[0073] At 536, the client node A 530 generates encrypted regulatory information of the confidential transaction by encrypting the transaction data using the public key of the regulator node 510, wherein the encrypted regulatory information is configured to allow decryption by the regulator node 510 using the private key corresponding to the public key.

[0074] In some implementations, the cryptographic commitment scheme includes the Pedersen Commitment scheme. In this case, generating one or more commitment values of a confidential transaction of the client node A 530 by applying a cryptographic commitment scheme to transaction data includes generating the one or more commitment values of the confidential transaction of the client node A 530 based on the transaction data and random numbers corresponding to the transaction data; and generating encrypted regulatory information of the confidential transaction includes generating encrypted regulatory information of the confidential transaction by encrypting the transaction data and random numbers corresponding to the transaction data using the public key of the regulator node.

[0075] At 538, the client node A 530 submits the content of the confidential transaction to the blockchain network for execution, for example, by transmitting the content of the confidential transaction to the blockchain node 520 (e.g., a consensus node of the blockchain network). In some implementations, the content of the confidential transaction can include: the one or more commitment values of the confidential transaction generated by the client node A 530 by applying the cryptographic commitment scheme to transaction data of the confidential transaction; the encrypted regulatory information

generated by the client node A 530 by encrypting the transaction data using the public key of the regulator node S 510; and one or more zero-knowledge proofs of the transaction data.

[0076] In some implementations, the one or more zero-knowledge proofs of the transaction data includes one or more zero-knowledge range proofs that values of the transaction data are within respective ranges. For example, the one or more zero-knowledge range proofs can include a zero-knowledge range proof that the account balance of the client node A 530 before the confidential transaction is larger than zero, a zero-knowledge range proof that the transaction amount of the confidential transaction is larger than zero, and a zero-knowledge range proof that the transaction amount is less than or equal to the account balance of the client node A 530 before the confidential transaction.

[0077] In some implementations, the one or more zero-knowledge proofs of the transaction data includes a zero-knowledge proof that the client node A 530 uses the public key of the regulator node 510 in generating the encrypted regulatory information of the confidential transaction.

[0078] In some implementations, the content of the confidential transaction further includes a digital signature of the client node A 530. In some implementations, the content of the confidential transaction can include additional or different information.

[0079] At 522, upon receiving the content of the confidential transaction, the blockchain node 520 can execute the confidential transaction, for example, by verifying that the confidential transaction is valid based on the content of the confidential transaction. In some implementations, verifying that the confidential transaction is valid based on the content of the confidential transaction can include one or more of: determining that the one or more commitment values are correct based on the commitment scheme and/or the one or more zero-knowledge proofs; or verifying the one or more zero-knowledge proofs of the transaction data, for example, according to algorithms as described with respect to FIG. 3.

[0080] At 524, after verifying the confidential transaction is valid, the blockchain node 520 can, for example, record the transaction (e.g., by storing the content of the confidential transaction in a blockchain on the blockchain network), and update account information effected by the confidential transaction (e.g., the account balance of the client node A 530 and client node B 540), for example, according to the techniques described with respect to FIG. 3 or other techniques.

[0081] At 516, the regulator node 510 obtains from the blockchain node 520 (e.g., a consensus node of the blockchain network) the content of the confidential transaction of the client node A 530. The content of the confidential transaction can include the example content 400 of the example confidential transaction 450 as described with respect to FIG. 4.

[0082] At 518, the regulator node 510 obtains the transaction data by decrypting the encrypted regulatory information using the private key of the regulator node.

[0083] At 519, the regulator node 510 verifies that the confidential transaction is legitimate based on the content of the confidential transaction and the transaction data. In some implementations, verifying that the confidential transaction is valid based on the content of the confidential transaction and the decrypted transaction data includes one or more of: determining that the one or more commitment values are correct based on the commitment scheme and/or the one or more zero-knowledge proofs; verifying the one or more zero-knowledge proofs of the transaction data; or determining that values of the transaction data comply with regulation.

[0084] In some implementations, verifying that one or more zero-knowledge proofs of the transaction data includes one or more of: determining that the account balance of the client node A 530 before the confidential transaction is larger than zero; determining that the transaction amount of the confidential transaction is larger than zero; or determining that a transaction amount of the confidential transaction is less than or equal to the account balance of the client node A 530 before the confidential transaction.

[0085] The features described may be implemented in digital electronic circuitry, or in computer hardware, firmware, software, or in combinations of them. The apparatus may be implemented in a computer program product tangibly embodied in an information carrier (e.g., in a machine-readable storage device) for execution by a programmable processor; and method steps may be performed by a programmable processor executing a program of instructions to perform functions of the described implementations by operating on input data and generating output. The described features may be implemented advantageously in one or more computer programs that are executable on a programmable system including at least one programmable processor coupled to receive data and instructions from, and to transmit data and instructions to, a data storage system, at least

one input device, and at least one output device. A computer program is a set of instructions that may be used, directly or indirectly, in a computer to perform a certain activity or bring about a certain result. A computer program may be written in any form of programming language, including compiled or interpreted languages, and it may be deployed in any form, including as a stand-alone program or as a module, component, subroutine, or other unit suitable for use in a computing environment.

[0086] Suitable processors for the execution of a program of instructions include, by way of example, both general and special purpose microprocessors, and the sole processor or one of multiple processors of any kind of computer. Generally, a processor will receive instructions and data from a read-only memory or a random access memory or both. Elements of a computer may include a processor for executing instructions and one or more memories for storing instructions and data. Generally, a computer may also include, or be operatively coupled to communicate with, one or more mass storage devices for storing data files; such devices include magnetic disks, such as internal hard disks and removable disks; magneto-optical disks; and optical disks. Storage devices suitable for tangibly embodying computer program instructions and data include all forms of non-volatile memory, including by way of example semiconductor memory devices, such as EPROM, EEPROM, and flash memory devices; magnetic disks such as internal hard disks and removable disks; magneto-optical disks; and CD-ROM and DVD-ROM disks. The processor and the memory may be supplemented by, or incorporated in, application-specific integrated circuits (ASICs).

[0087] To provide for interaction with a user, the features may be implemented on a computer having a display device such as a cathode ray tube (CRT) or liquid crystal display (LCD) monitor for displaying information to the user and a keyboard and a pointing device such as a mouse or a trackball by which the user may provide input to the computer.

[0088] The features may be implemented in a computer system that includes a back-end component, such as a data server, or that includes a middleware component, such as an application server or an Internet server, or that includes a front-end component, such as a client computer having a graphical user interface or an Internet browser, or any combination of them. The components of the system may be connected by any form or medium of digital data communication such as a communication network. Examples of

communication networks include, e.g., a local area network (LAN), a wide area network (WAN), and the computers and networks forming the Internet.

[0089] The computer system may include clients and servers. A client and server are generally remote from each other and typically interact through a network, such as the described one. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

[0090] In addition, the logic flows depicted in the figures do not require the particular order shown, or sequential order, to achieve desirable results. In addition, other steps may be provided, or steps may be eliminated, from the described flows, and other components may be added to, or removed from, the described systems. Accordingly, other implementations are within the scope of the following claims.

[0091] A number of implementations of the present disclosure have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the present disclosure. Accordingly, other implementations are within the scope of the following claims.

CLAIMS

1. A system comprising:

one or more computers; and

one or more computer-readable memories coupled to the one or more computers and having instructions stored thereon which are executable by the one or more computers to perform operations comprising:

generating, by a regulator node of a blockchain network, a pair of a public key and a private key;

publishing, by the regulator node, the public key to a plurality of client nodes of the blockchain network;

obtaining, by the regulator node from a consensus node of the blockchain network, a content of a confidential transaction of a client node, wherein the content of the confidential transaction comprises:

one or more commitment values of the confidential transaction generated by the client node by applying a cryptographic commitment scheme to transaction data of the confidential transaction;

one or more zero-knowledge proofs of the transaction data; and

encrypted regulatory information generated by the client node by encrypting the transaction data using the public key of the regulator node;

obtaining the transaction data by decrypting the encrypted regulatory information using the private key of the regulator node; and

verifying, by the regulator node, that the confidential transaction is legitimate based on the content of the confidential transaction and the transaction data.

2. The system of claim 1, wherein the transaction data of the confidential transaction comprises one or more of an account balance of the client node before the confidential transaction, or a transaction amount of the confidential transaction.

3. The system of claim 1, wherein the one or more zero-knowledge proofs of the transaction data comprises one or more zero-knowledge range proofs that values of the transaction data are within respective ranges.

4. The system of claim 1, wherein verifying that the confidential transaction is valid based on the content of the confidential transaction and the transaction data comprises one or more of:

determining that the one or more commitment values are correct based on the cryptographic commitment scheme;

verifying the one or more zero-knowledge proofs of the transaction data; or

determining that values of the transaction data comply with regulation.

5. The system of claim 4, wherein verifying the one or more zero-knowledge proofs of the transaction data comprises one or more of:

determining that an account balance of the client node before the confidential transaction is larger than zero;

determining that a transaction amount of the confidential transaction is larger than zero; and

determining that a transaction amount of the confidential transaction is less than or equal to an account balance of the client node before the confidential transaction.

6. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations:

generating, by a regulator node of a blockchain network, a pair of a public key and a private key;

publishing, by the regulator node, the public key to a plurality of client nodes of a blockchain network;

obtaining, by the regulator node from a consensus node of the blockchain network, a content of a confidential transaction of a client node, wherein the content of the confidential transaction comprises:

one or more commitment values of the confidential transaction generated by the client node by applying a cryptographic commitment scheme to transaction data of the confidential transaction;

one or more zero-knowledge proofs of the transaction data; and

encrypted regulatory information generated by the client node by encrypting the transaction data using the public key of the regulator node;

obtaining the transaction data by decrypting the encrypted regulatory information using the private key of the regulator node; and

verifying, by the regulator node, that the confidential transaction is legitimate based on the content of the confidential transaction and the transaction data.

7. The non-transitory, computer-readable medium of claim 6, wherein the transaction data of the confidential transaction comprises one or more of an account balance of the client node before the confidential transaction, or a transaction amount of the confidential transaction.

8. The non-transitory, computer-readable medium of claim 6, wherein the one or more zero-knowledge proofs of the transaction data comprises one or more zero-knowledge range proofs that values of the transaction data are within respective ranges.

9. The non-transitory, computer-readable medium of claim 6, wherein verifying that the confidential transaction is valid based on the content of the confidential transaction and the transaction data comprises one or more of:

determining that the one or more commitment values are correct based on the cryptographic commitment scheme;

verifying the one or more zero-knowledge proofs of the transaction data; or

determining that values of the transaction data comply with regulation.

10. The non-transitory, computer-readable medium of claim 9, wherein verifying the one or more zero-knowledge proofs of the transaction data comprises one or more of:

determining that an account balance of the client node before the confidential transaction is larger than zero;

determining that a transaction amount of the confidential transaction is larger than zero; and

determining that a transaction amount of the confidential transaction is less than or equal to an account balance of the client node before the confidential transaction.

11. A method comprising:

generating, by a regulator node of a blockchain network, a pair of a public key and a private key;

publishing, by the regulator node, the public key to a plurality of client nodes of the blockchain network;

obtaining, by a client node of the blockchain network, the public key of the regulator node;

generating, by the client node, one or more commitment values of a confidential transaction of the client node by applying a cryptographic commitment scheme to transaction data of the confidential transaction;

generating, by the client node, encrypted regulatory information of the confidential transaction by encrypting the transaction data using the public key of the regulator node; and

transmitting, by the client node to a consensus node of the blockchain network, a content of the confidential transaction for execution, wherein the content of the confidential transaction comprises:

the one or more commitment values;

the encrypted regulatory information; and

one or more zero-knowledge proofs of the transaction data;

obtaining, by the regulator node, the transaction data by decrypting the encrypted regulatory information using the private key of the regulator node; and

verifying, by the regulator node, that the confidential transaction is legitimate based on the content of the confidential transaction and the transaction data.

12. The method of claim 11, further comprising:

obtaining, by the regulator node from the consensus node of the blockchain network, the content of the confidential transaction of the client node.

13. The method of claim 11, wherein the transaction data of the confidential transaction comprises one or both of an account balance of the client node before the confidential transaction or a transaction amount of the confidential transaction.

14. The method of claim 11, wherein the one or more zero-knowledge proofs of the transaction data comprises one or more zero-knowledge range proofs that values of the transaction data are within respective ranges.

15. The method of claim 11, wherein the one or more zero-knowledge proofs of the transaction data comprises a zero-knowledge proof that the client node uses the public key of the regulator node in generating the encrypted regulatory information of the confidential transaction.

16. The method of claim 11, wherein the cryptographic commitment scheme comprises a Pedersen Commitment scheme;

wherein generating one or more commitment values of a confidential transaction of the client node by applying a cryptographic commitment scheme to transaction data comprises generating the one or more commitment values of the confidential transaction of the client node based on the transaction data and random numbers corresponding to the transaction data; and

wherein generating encrypted regulatory information of the confidential transaction comprises generating encrypted regulatory information of the confidential transaction by encrypting the transaction data and random numbers corresponding to the transaction data using the public key of the regulator node.

17. The method of claim 11, wherein the content of the confidential transaction further comprises a digital signature of the client node.

18. A system, comprising:

a client node; and

a regulator node comprising a memory and at least one processor,

wherein the regulator node is configured to perform operations comprising:

generating, by the regulator node of a blockchain network, a pair of a public key and a private key; and

publishing, by the regulator node, the public key to a plurality of client nodes of the blockchain network,

wherein the client node is configured to perform operations comprising:

obtaining the public key of the regulator node;

generating one or more commitment values of a confidential transaction of the client node by applying a cryptographic commitment scheme to transaction data of the confidential transaction;

generating, by the client node, encrypted regulatory information of the confidential transaction by encrypting the transaction data using the public key of the regulator node; and

transmitting, by the client node to a consensus node of the blockchain network, a content of the confidential transaction for execution, wherein the content of the confidential transaction comprises:

the one or more commitment values;

the encrypted regulatory information; and

one or more zero-knowledge proofs of the transaction data; and

wherein the regulator node is further configured to perform operations comprising:

obtaining the transaction data by decrypting the encrypted regulatory information using the private key of the regulator node; and

verifying, by the regulator node, that the confidential transaction is legitimate based on the content of the confidential transaction and the transaction data.

19. The system of claim 18, wherein the transaction data of the confidential transaction comprises one or both of an account balance of the client node before the confidential transaction or a transaction amount of the confidential transaction.

20. The system of claim 18, wherein the one or more zero-knowledge proofs of the transaction data comprises one or more zero-knowledge range proofs that values of the transaction data are within respective ranges.