

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 of the regulator node and a private key of the regulator node;
 - publishing, by the regulator node, the public key of the regulator node 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,
- 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.

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 of the regulator node and a private key of the regulator node;
 - publishing, by the regulator node, the public key of the regulator node 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, 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.

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 of the regulator node and a private key of the regulator node;

publishing, by the regulator node, the public key of the regulator node 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, 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.

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 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.

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

17. 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 of the regulator node and a private key of the regulator node; and
publishing, by the regulator node, the public key of the regulator node 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,
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.

18. The system of claim 17, 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.

19. The system of claim 17, 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.