CLAIMS:

1. A computer-implemented method for information protection, comprising:

determining one or more data inputs and one or more data outputs for a transaction, wherein the data inputs are associated with input data types respectively, and the data outputs are associated with output data types respectively;

encrypting the input data types and the output data types;

committing each of the encrypted input data types and the encrypted output data types with a commitment scheme to obtain corresponding commitment values, wherein the commitment scheme comprises a plurality of blinding factors respectively corresponding to the input data types and the output data types;

obtaining at least a parameter R based at least on the commitment values by:

obtaining differences between pairs of the commitment values,

concatenating the obtained differences,

encrypting the concatenated differences with a hash function to obtain an encryption value x, and

obtaining the parameter R based at least on the encryption value x and differences between pairs of the blinding factors; and

submitting the transaction to one or more nodes in a blockchain network with disclosure of the parameter R and without disclosure of the input data types and output data types for the nodes to verify consistency between the input data types and the output data types.

2. The method of claim 1, wherein: encrypting the input data types and the output data types comprises encrypting the input data types and the output data types with a hash function.

3. The method of claim 1, wherein: the commitment scheme comprises a Pedersen commitment.

4. The method of claim 1, wherein:

the commitment scheme comprises at least a blinding factor; and

the blinding factor changes with time of committing the encrypted input data types and the encrypted output data types.

5. The method of claim 1, wherein: the nodes are caused to verify the consistency between the input data types and the output data types without knowledge of the input data types and output data types.

6. The method of claim 1, wherein:

the transaction is based at least on an Unspent Transaction Outputs (UTXO) model; and

the data inputs and the data outputs comprise types of one or more assets undergoing the transaction.

7. The method of claim 1, wherein submitting the transaction to the one or more nodes in the blockchain network with disclosure of the parameter R and without disclosure of the input data types and output data types for the nodes to verify consistency between the input data types and the output data types comprises submitting the transaction to the one or more nodes in the blockchain network with disclosure of the parameter R and without disclosure of the input data types and output data types to cause the nodes to:

obtain the parameter R and a basepoint G;

obtain the differences between pairs of the commitment values;

concatenate the obtained differences;

encrypt the concatenated differences with a hash function to obtain an encryption value x;

obtain a sum C of polynomials based at least on the obtained differences and the encryption value x; and

in response to determining that the sum C is equal to a product of the parameter R and the basepoint G, determine that the input data types and the output data types are consistent; or

in response to determining that the sum C is not equal to a product of the parameter R and the basepoint G, determine that the input data types and the output data types are inconsistent.

8. A non-transitory computer-readable storage medium storing instructions to be executed by a processor to cause the processor to perform operations comprising:

determining one or more data inputs and one or more data outputs for a transaction, wherein the data inputs are associated with input data types respectively, and the data outputs are associated with output data types respectively;

encrypting the input data types and the output data types;

committing each of the encrypted input data types and the encrypted output data types with a commitment scheme to obtain corresponding commitment values, wherein the commitment scheme comprises a plurality of blinding factors respectively corresponding to the input data types and the output data types;

obtaining at least a parameter R based at least on the commitment values by:

obtaining differences between pairs of the commitment values,

concatenating the obtained differences,

encrypting the concatenated differences with a hash function to obtain an encryption value x, and

obtaining the parameter R based at least on the encryption value x and differences between pairs of the blinding factors; and

submitting the transaction to one or more nodes in a blockchain network with disclosure of the parameter R and without disclosure of the input data types and output data types for the nodes to verify consistency between the input data types and the output data types.

9. The storage medium of claim 8, wherein: encrypting the input data types and the output data types comprises encrypting the input data types and the output data types with a hash function.

10. The storage medium of claim 8, wherein: the commitment scheme comprises a Pedersen commitment.

11. The storage medium of claim 8, wherein:

the commitment scheme comprises at least a blinding factor; and

the blinding factor changes with time of committing the encrypted input data types and the encrypted output data types.

12. The storage medium of claim 8, wherein: the nodes are caused to verify the consistency between the input data types and the output data types without knowledge of the input data types and output data types.

13. The storage medium of claim 8, wherein:

the transaction is based at least on an Unspent Transaction Outputs (UTXO) model; and

the data inputs and the data outputs comprise types of one or more assets undergoing the transaction.

14. The storage medium of claim 8, wherein submitting the transaction to the one or more nodes in the blockchain network with disclosure of the parameter R and without disclosure of the input data types and output data types for the nodes to verify consistency between the input data types and the output data types comprises submitting the transaction to the one or more nodes in the blockchain network with disclosure of the parameter R and without disclosure of the input data types and output data types to cause the nodes to:

obtain the parameter R and a basepoint G;

obtain the differences between pairs of the commitment values;

concatenate the obtained differences;

encrypt the concatenated differences with a hash function to obtain an encryption value x;

obtain a sum C of polynomials based at least on the obtained differences and the encryption value x; and

in response to determining that the sum C is equal to a product of the parameter R and the basepoint G, determine that the input data types and the output data types are consistent; or

in response to determining that the sum C is not equal to a product of the parameter R and the basepoint G, determine that the input data types and the output data types are inconsistent.

15. A system for information protection, comprising a processor and a non-transitory computer-readable storage medium coupled to the processor, the storage

medium storing instructions to be executed by the processor to cause the system to perform operations comprising:

determining one or more data inputs and one or more data outputs for a transaction, wherein the data inputs are associated with input data types respectively, and the data outputs are associated with output data types respectively;

encrypting the input data types and the output data types;

committing each of the encrypted input data types and the encrypted output data types with a commitment scheme to obtain corresponding commitment values, wherein the commitment scheme comprises a plurality of blinding factors respectively corresponding to the input data types and the output data types;

obtaining at least a parameter R based at least on the commitment values by:

obtaining differences between pairs of the commitment values,

concatenating the obtained differences,

encrypting the concatenated differences with a hash function to obtain an encryption value x, and

obtaining the parameter R based at least on the encryption value x and differences between pairs of the blinding factors; and

submitting the transaction to one or more nodes in a blockchain network with disclosure of the parameter R and without disclosure of the input data types and output data types for the nodes to verify consistency between the input data types and the output data types.

16. A computer-implemented method for information protection, comprising:

obtaining, by one or more nodes in a blockchain network, a transaction initiated by an initiator node, wherein:

the transaction is associated with one or more data inputs and one or more data outputs,

the data inputs are respectively associated with input data types, and the data outputs are respectively associated with output data types respectively,

the input data types and the output data types are encrypted and committed to a commitment scheme to obtain corresponding commitment values, and

the input data types and output data types are not disclosed to the one or more nodes;

verifying, by the one or more nodes, consistency between the input data types and the output data types by:

obtaining a parameter R and a basepoint G,

obtaining differences between pairs of the commitment values,

concatenating the obtained differences,

encrypting the concatenated differences with a hash function to obtain an encryption value x,

obtaining a sum C of polynomials based at least on the obtained differences and the encryption value x, and

determining if the sum C is equal to a product of the parameter R and the basepoint G; and

in response to determining that the input data types and the output data types are consistent, adding, by the one or more nodes, the transaction to the blockchain network; or in response to determining that the input data types and the output data types are inconsistent, rejecting, by the one or more nodes, the transaction from being added to the blockchain network.

17. The method of claim 16, wherein verifying, by the one or more nodes, consistency between the input data types and the output data types further comprises:

in response to determining that the sum C is equal to the product of the parameter R and the basepoint G, determining that the input data types and the output data types are consistent; or

in response to determining that the sum C is not equal to the product of the parameter R and the basepoint G, determining that the input data types and the output data types are inconsistent.

18. A non-transitory computer-readable storage medium storing instructions to be executed by a processor to cause the processor to perform operations comprising:

obtaining, by one or more nodes in a blockchain network, a transaction initiated by an initiator node, wherein:

the transaction is associated with one or more data inputs and one or more data outputs,

the data inputs are respectively associated with input data types, and the data outputs are respectively associated with output data types respectively,

the input data types and the output data types are encrypted and committed to a commitment scheme to obtain corresponding commitment values, and

the input data types and output data types are not disclosed to the one or more nodes;

verifying, by the one or more nodes, consistency between the input data types and the output data types by:

obtaining a parameter R and a basepoint G,

obtaining differences between pairs of the commitment values,

concatenating the obtained differences,

encrypting the concatenated differences with a hash function to obtain an encryption value x,

obtaining a sum C of polynomials based at least on the obtained differences and the encryption value x, and

determining if the sum C is equal to a product of the parameter R and the basepoint G; and

in response to determining that the input data types and the output data types are consistent, adding, by the one or more nodes, the transaction to the blockchain network; or in response to determining that the input data types and the output data types are inconsistent, rejecting, by the one or more nodes, the transaction from being added to the blockchain network.

19. A system for information protection, comprising a processor and a non-transitory computer-readable storage medium coupled to the processor, the storage medium storing instructions to be executed by the processor to cause the system to perform operations comprising:

obtaining, by one or more nodes in a blockchain network, a transaction initiated by an initiator node, wherein:

the transaction is associated with one or more data inputs and one or more data outputs,

the data inputs are respectively associated with input data types, and the data outputs are respectively associated with output data types respectively,

the input data types and the output data types are encrypted and committed to a commitment scheme to obtain corresponding commitment values, and

the input data types and output data types are not disclosed to the one or more nodes;

verifying, by the one or more nodes, consistency between the input data types and the output data types by:

obtaining a parameter R and a basepoint G,

obtaining differences between pairs of the commitment values,

concatenating the obtained differences,

encrypting the concatenated differences with a hash function to obtain an encryption value x,

obtaining a sum C of polynomials based at least on the obtained differences and the encryption value x, and

determining if the sum C is equal to a product of the parameter R and the basepoint G; and

in response to determining that the input data types and the output data types are consistent, adding, by the one or more nodes, the transaction to the blockchain network; or in response to determining that the input data types and the output data types are inconsistent, rejecting, by the one or more nodes, the transaction from being added to the blockchain network.