CLAIMS:

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

committing, at a sender node of a sender of a transaction, a transaction amount t of the transaction with a first commitment scheme to obtain a transaction commitment value T, and committing, at the sender node, a change y of the transaction with a second commitment scheme to obtain a change commitment value Y, the first commitment scheme comprising a transaction blinding factor r_t, and the second commitment scheme comprising a change blinding factor r_y, wherein the transaction amount t is tapped from one or more assets A_1, A_2, …, A_k of the sender;

encrypting, at the sender node, a first combination of the change blinding factor r_y and the change y with a first key KA;

transmitting, by the sender node, the transaction blinding factor r_t, the transaction amount t, and the transaction commitment value T to a recipient node associated with a recipient of the transaction for the recipient node to verify the transaction;

in response to that the recipient node successfully verifies the transaction, obtaining, at the sender node, (1) an encrypted second combination of the transaction blinding factor r_t and the transaction amount t encrypted with a second key KB and (2) a signature SIGB associated with the encrypted second combination and the transaction commitment value T;

verifying, at the sender node, the signature SIGB;

in response to successfully verifying the signature SIGB, generating, at the sender node, a signature SIGA associated with the assets A_1, A_2, …, A_k, the encrypted first combination, the encrypted second combination, the transaction commitment value T, the change commitment value Y, and a difference between a sum of blinding factors corresponding to the assets A_1, A_2, …, A_k and a sum of the transaction blinding factor r_t and the change blinding factor r_y; and

transmitting, by the sender node, the assets A_1, A_2, …, A_k, the encrypted first combination and encrypted second combination, the transaction commitment value T, the change commitment value Y, the difference between the sum of blinding factors corresponding to the assets A_1, A_2, …, A_k and the sum of the transaction blinding factor r_t and the change blinding factor r_y, the signature SIGA, and the signature SIGB t to a plurality of nodes in a blockchain for the verification.

2. The method of claim 1, wherein:

the first commitment scheme comprises a Pedersen commitment based at least on the transaction blinding factor r_t and with the transaction amount t being a corresponding committed value; and

the second commitment scheme comprises a Pedersen commitment based at least on the change blinding factor r_y and with the change y being a corresponding committed value.

3. The method of claim 1, wherein transmitting the transaction blinding factor r_t, the transaction amount t, and the transaction commitment value T to the recipient node associated with the recipient of the transaction for the recipient node to verify the transaction comprises:

transmitting the transaction blinding factor r_t, the transaction amount t, and the transaction commitment value T to the recipient node associated with the recipient of the transaction, causing the recipient node to verify if the transaction commitment value T is equal to the first commitment scheme committing the transaction amount t with the transaction blinding factor r_t.

4. The method of claim 1, wherein:

obtaining the encrypted second combination and the signature SIGB comprises receiving from the recipient node (1) the encrypted second combination and (2) the signature SIGB associated with the encrypted second combination and the transaction commitment value T.

5. The method of claim 4, wherein:

each of the assets is associated with (1) a Pedersen commitment based at least on a blinding factor r_{ak} and a value of the each asset and (2) an encryption based at least on the blinding factor r_{ak} and the value of the each asset; and

the change y is a difference between the transaction amount t and the tapped assets.

6. The method of claim 1, wherein transmitting the encrypted first combination and the encrypted second combination to the plurality of nodes in the blockchain for the nodes in the blockchain to verify the transaction comprises:

transmitting the encrypted first combination and the encrypted second combination to the plurality of nodes in the blockchain, causing the nodes in the blockchain to, in response to successfully verifying the transaction, issue the transaction amount t to the recipient, eliminate the assets A_1, A_2, …, A_k, and issue the change y to the sender.

7. A non-transitory computer-readable storage medium storing instructions that, when executed by a processor, cause the processor to perform operations comprising:

committing, at a sender node of a sender of a transaction, a transaction amount t of the transaction with a first commitment scheme to obtain a transaction commitment value T, and committing, at the sender node, a change y of the transaction with a second commitment scheme to obtain a change commitment value Y, the first commitment scheme comprising a transaction blinding factor r_t, and the second commitment scheme comprising a change blinding factor r_y, wherein the transaction amount t is tapped from one or more assets A_1, A_2, …, A_k of the sender;

encrypting, at the sender node, a first combination of the change blinding factor r_y and the change y with a first key KA;

transmitting, by the sender node, the transaction blinding factor r_t, the transaction amount t, and the transaction commitment value T to a recipient node associated with a recipient of the transaction for the recipient node to verify the transaction;

in response to that the recipient node successfully verifies the transaction, obtaining, at the sender node, (1) an encrypted second combination of the transaction blinding factor r_t and the transaction amount t encrypted with a second key KB and (2) a signature SIGB associated with the encrypted second combination and the transaction commitment value T;

verifying, at the sender node, the signature SIGB;

in response to successfully verifying the signature SIGB, generating, at the sender node, a signature SIGA associated with the assets A_1, A_2, …, A_k, the encrypted first combination, the encrypted second combination, the transaction commitment value T, the change commitment value Y, and a difference between a sum of blinding factors corresponding to the assets A_1, A_2, …, A_k and a sum of the transaction blinding factor r_t and the change blinding factor r_y; and

transmitting, by the sender node, the assets A_1, A_2, …, A_k, the encrypted first combination, the encrypted second combination, the transaction commitment value T, the change commitment value Y, the difference between the sum of blinding factors corresponding to the

assets A_1, A_2, …, A_k and the sum of the transaction blinding factor r_t and the change blinding factor r_y, the signature SIGA, and the signature SIGB to a plurality of nodes in a blockchain for the verification.

8. The storage medium of claim 7, wherein:

the first commitment scheme comprises a Pedersen commitment based at least on the transaction blinding factor r_t and with the transaction amount t being a corresponding committed value; and

the second commitment scheme comprises a Pedersen commitment based at least on the change blinding factor r_y and with the change y being a corresponding committed value.

9. The storage medium of claim 7, wherein transmitting the transaction blinding factor r_t, the transaction amount t, and the transaction commitment value T to the recipient node associated with the recipient of the transaction for the recipient node to verify the transaction comprises:

transmitting the transaction blinding factor r_t, the transaction amount t, and the transaction commitment value T to the recipient node associated with the recipient of the transaction, causing the recipient node to verify if the transaction commitment value T is equal to the first commitment scheme committing the transaction amount t with the transaction blinding factor r_t.

10. The storage medium of claim 7, wherein:

obtaining the encrypted second combination and the signature SIGB comprises receiving from the recipient node the encrypted second combination and (2) the signature SIGB associated with the encrypted second combination and the transaction commitment value T.

11. The storage medium of claim 10, wherein:

each of the assets is associated with (1) a Pedersen commitment based at least on a blinding factor r_{ak} and a value of the each asset and (2) an encryption based at least on the blinding factor r_{ak} and the value of the each asset; and

the change y is a difference between the transaction amount t and the tapped assets.

12. The storage medium of claim 7, wherein transmitting the encrypted first combination and the encrypted second combination to the plurality of nodes in the blockchain for the nodes in the blockchain to verify the transaction comprises:

transmitting the encrypted first combination and the encrypted second combination to the plurality of nodes in the blockchain, causing the nodes in the blockchain to, in response to successfully verifying the transaction, issue the transaction amount t to the recipient, eliminate the assets A_1, A_2, …, A_k, and issue the change y to the sender.

13. 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 that, when executed by the processor, cause the system to perform operations comprising:

committing, at a sender node of a sender of a transaction, a transaction amount t of the transaction with a first commitment scheme to obtain a transaction commitment value T, and committing, at the sender node, a change y of the transaction with a second commitment scheme to obtain a change commitment value Y, the first commitment scheme comprising a transaction blinding factor r_t, and the second commitment scheme comprising a change blinding factor r_y, wherein the transaction amount t is tapped from one or more assets A_1, A_2, …, A_k of the sender;

encrypting, at the sender node, a first combination of the change blinding factor r_y and the change y with a first key KA;

transmitting, by the sender node, the transaction blinding factor r_t, the transaction amount t, and the transaction commitment value T to a recipient node associated with a recipient of the transaction for the recipient node to verify the transaction;

in response to that the recipient node successfully verifies the transaction, obtaining, at the sender node, (1) an encrypted second combination of the transaction blinding factor r_t and the transaction amount t encrypted with a second key KB and (2) a signature SIGB associated with the encrypted second combination and the transaction commitment value T;

verifying, at the sender node, the signature SIGB;

in response to successfully verifying the signature SIGB, generating, at the sender node, a signature SIGA associated with the assets A_1, A_2, …, A_k, the encrypted first combination, the encrypted second combination, the transaction commitment value T, the change commitment

value Y, and a difference between a sum of blinding factors corresponding to the assets A_1, A_2, …, A_k and a sum of the transaction blinding factor r_t and the change blinding factor r_y; and

transmitting, by the sender node, the assets A_1, A_2, …, A_k, the encrypted first combination and the encrypted second combination, the transaction commitment value T, the change commitment value Y, the difference between the sum of blinding factors corresponding to the assets A_1, A_2, …, A_k and the sum of the transaction blinding factor r_t and the change blinding factor r_y, the signature SIGA, and the signature SIGB to a plurality of nodes in a blockchain for verification.

14. The method of claim 1, wherein between transmitting, by the sender node, the transaction blinding factor r_t, the transaction amount t, and the transaction commitment value T to the recipient node and obtaining, at the sender node, (1) the encrypted second combination and (2) the signature SIGB, further comprising:

obtaining, at the recipient node, the transaction blinding factor r_t, the transaction amount t, and the transaction commitment value T from the sender node;

verifying, at the recipient node, the transaction based on the obtained transaction blinding factor r_t, the obtained transaction amount t, and the obtained transaction commitment value T;

in response to successfully verifying the transaction, encrypting, at the recipient node, a second combination of the transaction blinding factor r_t and the transaction amount t with the second key KB to obtain the encrypted second combination, and generating, at the recipient node, the signature SIGB representing that the recipient agrees to the encrypted second combination and the transaction commitment value T; and

transmitting, by the recipient node, the encrypted second combination and the signature SIGB to the sender node for verification.

15. The method of claim 14, wherein:

verifying the transaction based on the obtained transaction blinding factor r_t, the obtained transaction amount t, and the obtained transaction commitment value T comprises verifying if the obtained transaction commitment value T is equal to the first commitment scheme committing the obtained transaction amount t with the obtained transaction blinding factor r_t.

16. The non-transitory computer-readable storage medium of claim 7, wherein between transmitting, by the sender node, the transaction blinding factor r_t, the transaction amount t, and the transaction commitment value T to the recipient node and obtaining, at the sender node, (1) the encrypted second combination and (2) the signature SIGB, the operations further comprise:

obtaining, at the recipient node, the transaction blinding factor r_t, the transaction amount t, and the transaction commitment value T from the sender node;

verifying, at the recipient node, the transaction based on the obtained transaction blinding factor r_t, the obtained transaction amount t, and the obtained transaction commitment value T;

in response to successfully verifying the transaction, encrypting, at the recipient node, a second combination of the transaction blinding factor r_t and the transaction amount t with the second key KB to obtain the encrypted second combination, and generating, at the recipient node, the signature SIGB representing that the recipient agrees to the encrypted second combination and the transaction commitment value T; and

transmitting, by the recipient node, the encrypted second combination and the signature SIGB to the sender node for verification.

17. The system of claim 13, wherein between transmitting, by the sender node, the transaction blinding factor r_t, the transaction amount t, and the transaction commitment value T to the recipient node and obtaining, at the sender node, (1) the encrypted second combination and (2) the signature SIGB, the operations further comprise:

obtaining, at the recipient node, the transaction blinding factor r_t, the transaction amount t, and the transaction commitment value T from the sender node;

verifying, at the recipient node, the transaction based on the obtained transaction blinding factor r_t, the obtained transaction amount t, and the obtained transaction commitment value T;

in response to successfully verifying the transaction, encrypting, at the recipient node, a second combination of the transaction blinding factor r_t and the transaction amount t with the second key KB to obtain the encrypted second combination, and generating, at the recipient node, the signature SIGB representing that the recipient agrees to the encrypted second combination and the transaction commitment value T; and

transmitting, by the recipient node, the encrypted second combination and the signature to the sender node for verification.