CLAIMS:

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

obtaining a combination of a transaction blinding factor r_t and a transaction amount t encrypted with a public key PK_B of a recipient of a transaction, and obtaining a transaction commitment value T, wherein: the transaction amount t is committed with a commitment scheme by a sender node associated with a sender of the transaction to obtain the transaction commitment value T, the commitment scheme comprising at least the transaction blinding factor r_t;

decrypting the obtained combination with a private key SK_B of a recipient of the transaction to obtain the transaction blinding factor r_t and the transaction amount t; and

verifying the transaction based at least on the transaction commitment value T, the transaction blinding factor r_t, and the transaction amount t.

2. The method of claim 1, wherein: the public key PK_B of the recipient and the private key SK_B of the recipient are asymmetric encryption keys.

3. The method of claim 1, wherein: the commitment scheme comprises a Pedersen commitment based at least on the transaction blinding factor r_t and with the transaction amount t being a committed value.

4. The method of claim 1, wherein: the combination of the transaction blinding factor r_t and the transaction amount t comprises a concatenation of the transaction blinding factor r_t and the transaction amount t.

5. The method of claim 1, wherein: verifying the transaction based at least on the transaction commitment value T, the transaction blinding factor r_t, and the transaction amount t comprises:

in response to determining that the transaction commitment value T does not match the commitment scheme of the transaction amount t based on the transaction blinding factor r_t, rejecting the transaction; and

in response to determining that the transaction commitment value T matches the commitment scheme of the transaction amount t based on the transaction blinding factor r_t, approving the transaction by signing the transaction with the private key SK_B of the recipient to generate a recipient signature SIGB.

6. The method of claim 5, further comprising:

transmitting the transaction signed with the recipient signature SIGB to the sender node for the sender node to:

verify the recipient signature SIGB;

in response to successfully verifying the recipient signature SIGB, approve the transaction by signing the transaction with a private key SK_A of the sender to generate a sender signature SIGA, and submit information of the transaction to one or more nodes in a blockchain network for the one or more nodes to verify the transaction; and

in response to not successfully verifying the recipient signature SIGB, reject the transaction.

7. The method of claim 6, wherein the information of the transaction comprises:

the combination of the transaction blinding factor r_t and the transaction amount t encrypted with the public key PK_B of the recipient, another combination of the change blinding factor r_y and the change y encrypted with a public key PK_A of the sender, the transaction commitment value T, a change commitment value Y committing a change y of the transaction with the commitment scheme, the sender signature SIGA, and the recipient signature SIGB.

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

obtaining a combination of a transaction blinding factor r_t and a transaction amount t encrypted with a public key PK_B of a recipient of a transaction, and obtaining a transaction commitment value T, wherein: the transaction amount t is committed with a commitment scheme by a sender node associated with a sender of the transaction to obtain the transaction commitment value T, the commitment scheme comprising at least the transaction blinding factor r_t;

decrypting the obtained combination with a private key SK_B of a recipient of the transaction to obtain the transaction blinding factor r_t and the transaction amount t; and

verifying the transaction based at least on the transaction commitment value T, the transaction blinding factor r_t, and the transaction amount t.

9. The storage medium of claim 8, wherein: the public key PK_B of the recipient and the private key SK_B of the recipient are asymmetric encryption keys.

10. The storage medium of claim 8, wherein: the commitment scheme comprises a Pedersen commitment based at least on the transaction blinding factor r_t and with the transaction amount t being a committed value.

11. The storage medium of claim 8, wherein: the combination of the transaction blinding factor r_t and the transaction amount t comprises a concatenation of the transaction blinding factor r_t and the transaction amount t.

12. The storage medium of claim 8, wherein: verifying the transaction based at least on the transaction commitment value T, the transaction blinding factor r_t, and the transaction amount t comprises:

in response to determining that the transaction commitment value T does not match the commitment scheme of the transaction amount t based on the transaction blinding factor r_t, rejecting the transaction; and

in response to determining that the transaction commitment value T matches the commitment scheme of the transaction amount t based on the transaction blinding factor r_t, approving the transaction by signing the transaction with the private key SK_B of the recipient to generate a recipient signature SIGB.

13. The storage medium of claim 12, wherein the operations further comprise:

transmitting the transaction signed with the recipient signature SIGB to the sender node for the sender node to:

verify the recipient signature SIGB;

in response to successfully verifying the recipient signature SIGB, approve the transaction by signing the transaction with a private key SK_A of the sender to generate a sender signature SIGA, and submit information of the transaction to one or more nodes in a blockchain network for the one or more nodes to verify the transaction; and

in response to not successfully verifying the recipient signature SIGB, reject the transaction.

14. The storage medium of claim 13, wherein the information of the transaction comprises:

the combination of the transaction blinding factor r_t and the transaction amount t encrypted with the public key PK_B of the recipient, another combination of the change blinding factor r_y and the change y encrypted with a public key PK_A of the sender, the transaction commitment value T, a change commitment value Y committing a change y of the transaction with the commitment scheme, the sender signature SIGA, and the recipient signature SIGB.

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:

obtaining a combination of a transaction blinding factor r_t and a transaction amount t encrypted with a public key PK_B of a recipient of a transaction, and obtaining a transaction commitment value T, wherein: the transaction amount t is committed with a commitment scheme by a sender node associated with a sender of the transaction to obtain the transaction commitment value T, the commitment scheme comprising at least the transaction blinding factor r_t;

decrypting the obtained combination with a private key SK_B of a recipient of the transaction to obtain the transaction blinding factor r_t and the transaction amount t; and

verifying the transaction based at least on the transaction commitment value T, the transaction blinding factor r_t, and the transaction amount t.

16. The system of claim 15, wherein: the public key PK_B of the recipient and the private key SK_B of the recipient are asymmetric encryption keys.

17. The system of claim 15, wherein: the commitment scheme comprises a Pedersen commitment based at least on the transaction blinding factor r_t and with the transaction amount t being a committed value.

18. The system of claim 15, wherein: the combination of the transaction blinding factor r_t and the transaction amount t comprises a concatenation of the transaction blinding factor r_t and the transaction amount t.

19. The system of claim 15, wherein: verifying the transaction based at least on the transaction commitment value T, the transaction blinding factor r_t, and the transaction amount t comprises:

in response to determining that the transaction commitment value T does not match the commitment scheme of the transaction amount t based on the transaction blinding factor r_t, rejecting the transaction; and

in response to determining that the transaction commitment value T matches the commitment scheme of the transaction amount t based on the transaction blinding factor r_t, approving the transaction by signing the transaction with the private key SK_B of the recipient to generate a recipient signature SIGB.

20. The system of claim 19, wherein the operations further comprise:

transmitting the transaction signed with the recipient signature SIGB to the sender node for the sender node to:

verify the recipient signature SIGB;

in response to successfully verifying the recipient signature SIGB, approve the transaction by signing the transaction with a private key SK_A of the sender to generate a sender signature SIGA, and submit information of the transaction to one or more nodes in a blockchain network for the one or more nodes to verify the transaction; and

in response to not successfully verifying the recipient signature SIGB, reject the transaction.