

CLAIMS:

1. A computer-implemented method for information protection, comprising:
committing a transaction amount t of a transaction with a commitment scheme to obtain a transaction commitment value T , the commitment scheme comprising at least a transaction blinding factor r_t ;

encrypting a combination of the transaction blinding factor r_t and the transaction amount t with a public key PK_B of a recipient of the transaction; and

transmitting the transaction commitment value T and the encrypted combination to a recipient node associated with the recipient for the recipient node to verify the transaction.

2. The method of claim 1, wherein: the public key PK_B is an asymmetric encryption key.

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 transmitting the transaction commitment value T and the encrypted combination to the recipient node associated with the recipient for the recipient node to verify the transaction comprises transmitting the transaction commitment value T and the encrypted combination to the recipient node associated with the recipient, causing the recipient node to:

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

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

6. The method of claim 5, wherein causing the recipient node to verify the transaction based at least on the transaction commitment value T , the transaction blinding factor r_t , and the transaction amount t comprises causing the recipient node to:

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 , reject 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 , approve the transaction by signing the transaction with the private key SK_B of the recipient to generate a recipient signature $SIGB$.

7. The method of claim 6, before transmitting the encrypted combination to the recipient node associated with the recipient, further comprising:

committing a change y of the transaction with the commitment scheme to obtain a change commitment value Y , the commitment scheme comprising at least a change blinding factor r_y , wherein the change y is one or more assets of a sender of the transaction that are tapped for the transaction less the transaction amount t ; and

encrypting another combination of the change blinding factor r_y and the change y with a public key PK_A of the sender.

8. The method of claim 7, further comprising:

in response to receiving the recipient signature $SIGB$, approving the transaction by signing the transaction with a private key SK_A of the sender to generate a sender signature $SIGA$; and

submitting the transaction comprising the encrypted combination, the encrypted another combination, the transaction commitment value T , the change commitment value Y , the sender signature $SIGA$, and the recipient signature $SIGB$ to one or more nodes in a blockchain network for the one or more nodes to verify the transaction.

9. The method of claim 8, wherein submitting the transaction comprising the encrypted combination, the encrypted another combination, the transaction

commitment value T , the change commitment value Y , the sender signature $SIGA$, and the recipient signature $SIGB$ to the one or more nodes in the blockchain network for the one or more nodes to verify the transaction comprises:

submitting the transaction comprising the encrypted combination, the encrypted another combination, the transaction commitment value T , the change commitment value Y , the sender signature $SIGA$, and the recipient signature $SIGB$ to the one or more nodes in the blockchain network, causing the one or more nodes to, in response to successfully verifying the transaction, issue the transaction amount t to the recipient, eliminate the one or more assets tapped for the transaction, and issue the change y to the sender.

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

committing a transaction amount t of a transaction with a commitment scheme to obtain a transaction commitment value T , the commitment scheme comprising at least a transaction blinding factor r_t ;

encrypting a combination of the transaction blinding factor r_t and the transaction amount t with a public key PK_B of a recipient of the transaction; and

transmitting the transaction commitment value T and the encrypted combination to a recipient node associated with the recipient for the recipient node to verify the transaction.

11. The storage medium of claim 10, wherein: the public key PK_B is an asymmetric encryption key.

12. The storage medium of claim 10, 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.

13. The storage medium of claim 10, 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 .

14. The storage medium of claim 10, wherein transmitting the transaction commitment value T and the encrypted combination to the recipient node associated with the recipient for the recipient node to verify the transaction comprises transmitting the transaction commitment value T and the encrypted combination to the recipient node associated with the recipient, causing the recipient node to:

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

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

15. The storage medium of claim 14, wherein causing the recipient node to verify the transaction based at least on the transaction commitment value T , the transaction blinding factor r_t , and the transaction amount t comprises causing the recipient node to:

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 , reject 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 , approve the transaction by signing the transaction with the private key SK_B of the recipient to generate a recipient signature SIG_B .

16. The storage medium of claim 15, before transmitting the encrypted combination to the recipient node associated with the recipient, the operations further comprise:

committing a change y of the transaction with the commitment scheme to obtain a change commitment value Y , the commitment scheme comprising at least a change blinding factor r_y , wherein the change y is one or more assets of a sender of the transaction that are tapped for the transaction less the transaction amount t ; and

encrypting another combination of the change blinding factor r_y and the change y with a public key PK_A of the sender.

17. The storage medium of claim 16, wherein the operations further comprise:

in response to receiving the recipient signature SIGB, approving the transaction by signing the transaction with a private key SK_A of the sender to generate a sender signature SIGA; and

submitting the transaction comprising the encrypted combination, the encrypted another combination, the transaction commitment value T, the change commitment value Y, the sender signature SIGA, and the recipient signature SIGB to one or more nodes in a blockchain network for the one or more nodes to verify the transaction.

18. The storage medium of claim 17, wherein submitting the transaction comprising the encrypted combination, the encrypted another combination, the transaction commitment value T, the change commitment value Y, the sender signature SIGA, and the recipient signature SIGB to the one or more nodes in the blockchain network for the one or more nodes to verify the transaction comprises:

submitting the transaction comprising the encrypted combination, the encrypted another combination, the transaction commitment value T, the change commitment value Y, the sender signature SIGA, and the recipient signature SIGB to the one or more nodes in the blockchain network, causing the one or more nodes to, in response to successfully verifying the transaction, issue the transaction amount t to the recipient, eliminate the one or more assets tapped for the transaction, and issue the change y to the sender.

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:

committing a transaction amount t of a transaction with a commitment scheme to obtain a transaction commitment value T, the commitment scheme comprising at least a transaction blinding factor r_t ;

encrypting a combination of the transaction blinding factor r_t and the transaction amount t with a public key PK_B of a recipient of the transaction; and

transmitting the transaction commitment value T and the encrypted combination to a recipient node associated with the recipient for the recipient node to verify the transaction.

20. 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 .

21. The method of claim 20, wherein: the public key PK_B of the recipient and the private key SK_B of the recipient are asymmetric encryption keys.

22. 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 .

23. 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 .