instructions for processor(s) 504. A storage device 510, such as a magnetic disk, optical disk, or USB thumb drive (Flash drive), etc., is provided and coupled to bus 502 for storing information and instructions.

[125] The computer system 500 may implement the techniques described herein using customized hard-wired logic, one or more ASICs or FPGAs, firmware and/or program logic which in combination with the computer system causes or programs computer system 500 to be a special-purpose machine. According to one embodiment, the operations, methods, and processes described herein are performed by computer system 500 in response to processor(s) 504 executing one or more sequences of one or more instructions contained in main memory 506. Such instructions may be read into main memory 506 from another storage medium, such as storage device 510. Execution of the sequences of instructions contained in main memory 506 causes processor(s) 504 to perform the process steps described herein. In alternative embodiments, hard-wired circuitry may be used in place of or in combination with software instructions.

[126] The main memory 506, the ROM 508, and/or the storage device 510 may include non-transitory storage media. The term "non-transitory media," and similar terms, as used herein refers to media that store data and/or instructions that cause a machine to operate in a specific fashion, the media excludes transitory signals. Such non-transitory media may comprise non-volatile media and/or volatile media. Non-volatile media includes, for example, optical or magnetic disks, such as storage device 510. Volatile media includes dynamic memory, such as main memory 506. Common forms of non-transitory media include, for example, a floppy disk, a flexible disk, hard disk, solid state drive, magnetic tape, or any other magnetic data storage medium, a CD-ROM, any other optical data storage medium, any physical medium with patterns of holes, a RAM, a PROM, and EPROM, a FLASH-EPROM, NVRAM, any other memory chip or cartridge, and networked versions of the same.

[127] The computer system 500 also includes a network interface 518 coupled to bus 502. Network interface 518 provides a two-way data communication coupling to one or more network links that are connected to one or more local networks. For example, network interface 518 may be an integrated services digital network (ISDN) card, cable modem, satellite modem, or a modem to provide a data communication

CLAIMS:

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

committing a transaction amount t of a transaction with a first commitment scheme to obtain a transaction commitment value T, and committing 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;

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

transmitting 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 an encrypted second combination of the transaction blinding factor r_t and the transaction amount t encrypted with a second key KB; and

transmitting the encrypted first combination and the encrypted second combination to a plurality of nodes in a blockchain for the nodes in the blockchain to verify the transaction.

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 comprises receiving from the recipient node the encrypted second combination and a signature SIGB associated with the encrypted second combination and the transaction commitment value T.

5. The method of claim 4, wherein:

the transaction amount t is tapped from one or more assets A_1, A_2, ..., A_k of a sender of the transaction;

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 5, wherein, before transmitting the encrypted first combination and the encrypted second combination to the plurality of nodes in the blockchain, further comprising:

verifying the signature SIGB; and

in response to successfully verifying the signature SIGB, generating a signature SIGA associated with the assets A_1, A_2, ..., A_k, the first combination, the 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.

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

transmitting the assets A_1, A_2, ..., A_k, the first combination, the second combination, the transaction commitment value T, the change commitment value Y, 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, the signature SIGA, and the signature SIGB to the plurality of nodes in the blockchain.

8. The method 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.

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

committing a transaction amount t of a transaction with a first commitment scheme to obtain a transaction commitment value T, and committing 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;

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

transmitting 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 an encrypted second combination of the transaction blinding factor r_t and the transaction amount t encrypted with a second key KB; and

transmitting the encrypted first combination and the encrypted second combination to a plurality of nodes in a blockchain for the nodes in the blockchain to verify the transaction.

10. The storage medium of claim 9, 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.

11. The storage medium of claim 9, 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.

12. The storage medium of claim 9, wherein:

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

13. The storage medium of claim 12, wherein:

the transaction amount t is tapped from one or more assets $A_1, A_2, \ldots, A_k$ of a sender of the transaction;

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.

14. The storage medium of claim 13, wherein, before transmitting the encrypted first combination and the encrypted second combination to the plurality of nodes in the blockchain, the operations further comprise:

verifying the signature SIGB; and

in response to successfully verifying the signature SIGB, generating a signature SIGA associated with the assets A_1, A_2, ..., A_k, the first combination, the 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.

15. The storage medium of claim 14, wherein transmitting the encrypted first combination and the encrypted second combination to the plurality of nodes in the blockchain comprises:

transmitting the assets A_1, A_2, ..., A_k, the first combination, the second combination, the transaction commitment value T, the change commitment value Y, 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, the signature SIGA, and the signature SIGB to the plurality of nodes in the blockchain.

16. The storage medium of claim 15, 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.

17. 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 a transaction amount t of a transaction with a first commitment scheme to obtain a transaction commitment value T, and committing 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 rt, and the second commitment scheme comprising a change blinding factor ry;

encrypting a first combination of the change blinding factor ry and the change y with a first key KA;

transmitting the transaction blinding factor rt, 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 an encrypted second combination of the transaction blinding factor rt and the transaction amount t encrypted with a second key KB; and

transmitting the encrypted first combination and the encrypted second combination to a plurality of nodes in a blockchain for the nodes in the blockchain to verify the transaction.

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

obtaining a transaction blinding factor rt, a transaction amount t of a transaction, and a transaction commitment value T from a sender node associated with a sender of a transaction, wherein: the transaction amount t is committed with a first commitment scheme to obtain the transaction commitment value T, the first commitment scheme comprising the transaction blinding factor rt;

verifying the transaction based on the obtained transaction blinding factor rt, the obtained transaction amount t of a transaction, and the obtained transaction commitment value T;

in response to successfully verifying the transaction, encrypting a second combination of the transaction blinding factor rt and the transaction amount t encrypted with a second key KB; and

transmitting the encrypted second combination to the sender node.

19. The method of claim 18, wherein:

verifying the transaction based on the obtained transaction blinding factor rt, the obtained transaction amount t of a transaction, 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 rt.

20. The method of claim 18, wherein:

before transmitting the encrypted second combination to the sender node, further comprising generating a signature SIGB associated with the encrypted second combination and the transaction commitment value T; and

transmitting the encrypted second combination to the sender node comprises transmitting the encrypted second combination and the signature SIGB to the sender node.

21. The method of claim 18, wherein:

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

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

obtaining a transaction blinding factor r_t, a transaction amount t of a transaction, and a transaction commitment value T from a sender node associated with a sender of a transaction, wherein: the transaction amount t is committed with a first commitment scheme to obtain the transaction commitment value T, the first commitment scheme comprising the transaction blinding factor r_t;

verifying the transaction based on the obtained transaction blinding factor r_t, the obtained transaction amount t of a transaction, and the obtained transaction commitment value T;

in response to successfully verifying the transaction, encrypting a second combination of the transaction blinding factor r_t and the transaction amount t with a second key KB; and

transmitting the encrypted second combination to the sender node.

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

obtaining a transaction blinding factor r_t, a transaction amount t of a transaction, and a transaction commitment value T from a sender node associated with a sender of a transaction, wherein: the transaction amount t is committed with a first commitment scheme to obtain the transaction commitment value T, the first commitment scheme comprising the transaction blinding factor r_t;

verifying the transaction based on the obtained transaction blinding factor r_t, the obtained transaction amount t of a transaction, and the obtained transaction commitment value T;

in response to successfully verifying the transaction, encrypting a second combination of the transaction blinding factor r_t and the transaction amount t with a second key KB; and

transmitting the encrypted second combination to the sender node.