

the nodes delete the transferred asset from the paying wallet and add a corresponding asset to a recipient wallet.

[55] However, limitations still exist for such scheme. First, the scheme requires the user to maintain a persistent storage locally to manage the random numbers and plaintext balances corresponding to the encrypted account balance, and the management implementation is complicated; second, the storage of blinding factors (e.g., the random numbers) and the plaintext balances corresponding to the “Pedersen asset” in a single local node is prone to loss or corruption, while multi-node backup storage is difficult to realize due to the frequent change of the account balance.

[56] The systems and method presented in this disclosure may overcome the above limitations and achieve robust privacy protection for transaction amounts, asset values, and blinding factors in commitment schemes. To that end, the symmetric keys obtained by Diffie-Hellman (DH) key exchange protocol may be used to encrypt/decrypt the random numbers and the plaintext balances, thus providing convenient management. Further, storing the encrypted information in blockchain ensures that the transaction amounts, asset values, and blinding factors in commitment schemes are not easily lost or tampered with.

[57] Before discussing the figures of this disclosure, the Pedersen Commitment and Diffie-Hellman (DH) key exchange protocol are described below.

[58] In some embodiments, a commitment scheme (e.g., Pedersen commitment) may encrypt certain value a (e.g., transaction amount, asset value, key parameter) as follows:

$$PC(a) = r \times G + a \times H$$

[59] where r is a random blinding factor (alternatively referred to as binding factor) that provides hiding, G and H are the publicly agreed generators/basepoints of the elliptic curve and may be chosen randomly, a is the value of the commitment, $PC(a)$ is the curve point used as commitment and given to the counterparty, and H is another curve point. That is, G and H may be known parameters to nodes. A “nothing up my sleeve” generation of H may be generated by hashing the basepoint

CLAIMS:

1. A computer-implemented method for information protection, comprising:
obtaining, by a recipient node associated with a recipient of a transaction from a sender node associated with a sender of the transaction:

- i) a combination of a transaction blinding factor r_t and a transaction amount t encrypted with a first key of a symmetric key pair, wherein the first key is generated by the sender node based on a public key PK_B of the recipient; and
- ii) a transaction commitment value T generated by the sender node committing the transaction amount t according to a commitment scheme based on the transaction blinding factor r_t ;

generating, by the recipient node, a second key of the symmetric key pair based on a public key PK_A of the sender;

decrypting, by the recipient node, the obtained combination with the second key to obtain the transaction blinding factor r_t and the transaction amount t ;

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

in response to successfully verifying the transaction, generating, by the recipient node, a recipient signature SIG_B representing that the recipient has approved the transaction; and

transmitting, by the recipient node, the recipient signature SIG_B to the sender node.

2. The method of claim 1, wherein generating the second key of the symmetric key pair comprises generating the second key of the symmetric key pair based on both a private key SK_B of the recipient and the public key PK_A of the sender under a Diffie-Hellman key exchange protocol.

3. The method of claim 2, wherein the commitment scheme comprises a Pedersen commitment with the transaction amount t being a committed value.

4. The method of claim 1, wherein:

the first key is generated by the sender node based on a private key SK_A of the sender of the transaction and the public key PK_B of the recipient of the transaction.

5. 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 .

6. 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:

determining whether the transaction commitment value T matches a commitment of the transaction amount t according to the commitment scheme based on the transaction blinding factor r_t ;

7. The method of claim 1, wherein transmitting the recipient signature SIG_B to the sender node comprises transmitting the transaction signed with the recipient signature SIG_B to the sender node for the sender node to:

verify the recipient signature SIG_B ; and

(i) in response to successfully verifying the recipient signature SIG_B , approve the transaction by signing the transaction with a private key SK_A of the sender to generate a sender signature SIG_A , 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, or (ii) in response to not successfully verifying the recipient signature SIG_B , reject the transaction.

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

the combination of the transaction blinding factor r_t and the transaction amount t encrypted with the first key of the symmetric key pair, another combination of a change blinding factor r_y and a change y encrypted with another key generated based on the private key SK_A and the public key PK_A of the sender, the transaction commitment value T , a change commitment value Y committing the change y of the transaction with the commitment scheme, the sender signature SIG_A , and the recipient signature SIG_B .

9. A computer-implemented method for information protection, comprising:
obtaining, by a recipient node associated with a recipient of a transaction from a sender node associated with a sender of the transaction:

- i) a combination of a transaction blinding factor r_t and a transaction amount t encrypted with a first key of a symmetric key pair; and
- ii) a transaction commitment value T generated by the sender node committing the transaction amount t according to a commitment scheme based on the transaction blinding factor r_t ;

generating, by the recipient node, a second key of the symmetric key pair;
decrypting, by the recipient node, the obtained combination with the second key to obtain the transaction blinding factor r_t and the transaction amount t ;

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

in response to successfully verifying the transaction, generating, by the recipient node, a recipient signature SIG_B representing that the recipient has approved the transaction; and

transmitting, by the recipient node, the recipient signature SIG_B to the sender node for the sender node to:

verify the recipient signature SIG_B ; and

in response to successfully verifying the recipient signature SIG_B , approve the transaction by signing the transaction with a private key SK_A of the sender to generate a sender signature SIG_A , 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, wherein the information of the transaction comprises:

the combination of the transaction blinding factor r_t and the transaction amount t encrypted with the first key of the symmetric key pair, another combination of a change blinding factor r_y and a change y encrypted with another key generated based on the private key SK_A and the public key PK_A of the sender, the transaction commitment value T , a change commitment

value Y committing the change y of the transaction with the commitment scheme, the sender signature SIGA, and the recipient signature SIGB.

10. A non-transitory computer-readable storage medium storing instructions to be executed by a processor to cause the processor to perform the method of any one of claims 1 to 9.

11. 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 the method of any one of claims 1 to 9.