

homomorphic encryption 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.

[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 G with a hash function mapping from a point to another with $H = \text{Hash}(G)$. H and G are the public parameters of the given system (e.g., randomly generated points on an elliptic curve). Although the above provides an example of Pedersen commitment in elliptic curve form, various other forms of Pedersen commitment or other commitment schemes may be alternatively used.

[60] A commitment scheme maintains data secrecy but commits to the data so that it cannot be changed later by the sender of the data. If a party only knows the commitment value (e.g., $PC(a)$), they cannot determine what underlying data values (e.g., a) have been committing to. Both the data (e.g., a) and the blinding factor (e.g., r) may be revealed later (e.g., by the initiator node), and a recipient (e.g., consensus node) of the commitment can run the commitment and verify that the committed data matches the revealed data. The blinding factor is present because without one, someone could try guessing at the data.

[61] Commitment schemes are a way for the sender (committing party) to commit to a value (e.g., a) such that the value committed remains private, but can be revealed at a later time when the committing party divulges a necessary parameter

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 via an off-blockchain channel, a combination of a transaction blinding factor r_t and a transaction amount t encrypted with a public key PK_{2_B} of the recipient of the transaction, and a transaction commitment value T generated by the sender node committing the transaction amount t with a commitment scheme based at least on the transaction blinding factor r_t ; wherein recipient is associated with a different public key PK_{1_B} as an address for receiving the transaction amount t ;

decrypting, by the recipient node, the obtained combination with a private key SK_{2_B} of the recipient of the transaction to obtain the transaction blinding factor r_t and the transaction amount t , wherein the public key PK_{2_B} and the private key SK_{2_B} are a public-private key pair of the recipient;

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 ; and

in response to determining that the transaction commitment value T matches the commitment scheme corresponding to committing the transaction amount t based on the transaction blinding factor r_t , approving, by the recipient node, the transaction by signing the transaction with a different private key SK_{1_B} of the recipient of the recipient to transmit to the sender node, wherein the different public key PK_{1_B} and the different private key SK_{1_B} are a different public-private key pair of the recipient.

2. The method of claim 1, wherein the public key PK_{2_B} of the recipient and the private key SK_{2_B} of the recipient are a homomorphic encryption key pair.

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:

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 ;

6. The method of claim 1, wherein:

signing the transaction with the different private key SK_{1_B} of the recipient generates a recipient signature $SIGB$; and

the method further comprises transmitting, by the recipient node, the recipient signature $SIGB$ to the sender node.

7. The method of claim 6, wherein: transmitting the transaction signed with the recipient signature $SIGB$ to the sender node comprises transmitting the recipient signature $SIGB$ to the sender node for the sender node to:

verify the recipient signature $SIGB$; and

(i) in response to successfully verifying the recipient signature $SIGB$, approve the transaction by signing the transaction with a private key SK_{1_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, or (ii) in response to not successfully verifying the recipient signature $SIGB$, 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 second public key PK_{2_B} of the recipient of the transaction, another combination of the change blinding factor r_y and the change y encrypted with a second public key PK_{2_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 $SIGB$.

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 via an off-blockchain channel, a combination of a transaction blinding factor r_t and a transaction amount t encrypted with a public key PK_{2_B} of the recipient of the transaction, and a transaction commitment value T generated by the sender node committing the transaction amount t with a commitment scheme based at least on the transaction blinding factor r_t ;

decrypting, by the recipient node, the obtained combination with a private key SK_{2_B} of the recipient of the transaction to obtain the transaction blinding factor r_t and the transaction amount t , wherein the public key PK_{2_B} and the private key SK_{2_B} are a public-private key pair of the recipient;

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 determining that the transaction commitment value T matches the commitment scheme corresponding to committing the transaction amount t based on the transaction blinding factor r_t , approving, by the recipient node, the transaction by signing the transaction with a private key SK_{1_B} of the recipient to generate a recipient signature $SIGB$; and

transmitting, by the recipient node, the recipient signature $SIGB$ to the sender node for the sender node to:

verify the recipient signature $SIGB$; and

in response to successfully verifying the recipient signature $SIGB$, approve the transaction by signing the transaction with a private key SK_{1_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, wherein the information of the transaction comprises:

the combination of the transaction blinding factor r_t and the transaction amount t encrypted with the second public key PK_{2_B} of the recipient of the transaction, another combination of the change blinding factor r_y and the change y encrypted with a second public key PK_{2_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.

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.