

## CLAIMS

1. A method for providing data privacy in a private distributed ledger, comprising:
  - a distributed application preparing a transaction payload for a private transaction;
  - the distributed application sending a payload storage message comprising a hash digest, an encrypted payload, and an encrypted symmetric key to a transaction key manager;
  - the transaction key manager storing the hash and the encrypted payload;
  - the distributed application sending a pending transaction comprising the hash digest to one of a plurality of nodes, wherein the pending transaction is identified as private by a sentinel byte;
  - one of the plurality of nodes proposing a block comprising the pending transaction to the other nodes;
  - each of the plurality of nodes validating the pending transaction in the block by identifying the pending transaction as a private transaction; and
  - one of the plurality of nodes sending a transaction payload request message to a transaction key manager associated with the node.
2. A method of claim 1, wherein the pending transaction is identified as private by a flag in a body of the pending transaction.
3. The method of claim 1, wherein the step of preparing a transaction payload for a private transaction comprises:
  - generating the symmetric key;
  - encrypting the payload with the symmetric key;
  - calculating the hash digest of the encrypted payload; and
  - encrypting the symmetric key with public keys of parties to the transaction.

4. The method of claim 1, wherein the transaction payload request message comprises the node's public key, the hash digest, and the node's signature.

5. The method of claim 1, further comprising:

the transaction key manager returning a decrypted payload and encrypted symmetric key to one of the nodes in response to the node being a party to the transaction.

6. The method of claim 1, further comprising:

the transaction key manager returning an indication to one of the nodes that the transaction is private in response to the node not being a party to the transaction.

7. A method for providing data privacy in a private distributed ledger, comprising:

a distributed application preparing a transaction payload for a private transaction;

the distributed application sending a payload storage message comprising a hash digest, an encrypted payload, and an encrypted symmetric key to a transaction key manager;

the transaction key manager storing the hash and the encrypted payload;

the distributed application sending a pending transaction comprising the hash digest to one of a plurality of nodes, wherein the pending transaction is identified as private by a flag in a body of the pending transaction;

one of the plurality of nodes proposing a block comprising the pending transaction to the other nodes;

- each of the plurality of nodes validating the pending transaction in the block by identifying the pending transaction as a private transaction; and
- one of the plurality of nodes sending a transaction payload request message to a transaction key manager associated with the node.
8. The method of claim 7, wherein the step of preparing a transaction payload for a private transaction comprises:
- generating the symmetric key;
  - encrypting the payload with the symmetric key;
  - calculating the hash digest of the encrypted payload; and
  - encrypting the symmetric key with public keys of parties to the transaction.
9. The method of claim 7, wherein the transaction payload request message comprises the node's public key, the hash digest, and the node's signature.
10. The method of claim 7, further comprising:
- the transaction key manager returning a decrypted payload and encrypted symmetric key to one of the nodes in response to the node being a party to the transaction.
11. The method of claim 7, further comprising:
- the transaction key manager returning an indication to one of the nodes that the transaction is private in response to the node not being a party to the transaction.