CLAIMS

1. A system, comprising:

a distributed ledger comprising a plurality of nodes; and

at least one application executable by at least one of the plurality of nodes, wherein, when executed by the at least one of the plurality of nodes, the at least one application causes the at least one of the plurality of nodes to at least:

receive authorization confirmation data and a first non-interactive zero-knowledge proof from a first entity following a second entity authorizing a transaction for the first entity, the first entity corresponding to a merchant, the second entity corresponding to an issuer, wherein the authorization confirmation data comprises a hashed memo comprising encrypted data that describes the transaction;

validate the authorization confirmation data by using the first non-interactive zero-knowledge proof to verify at least one factor of the authorization confirmation data that is encrypted in the hashed memo;

write the authorization confirmation data to the distributed ledger;

receive payment confirmation data and a second non-interactive zero-knowledge proof from the second entity following the second entity providing a payment associated with the transaction to the first entity, the payment confirmation data corresponding to a hash of a transaction confirmation identifier for the transaction;

validate the payment confirmation data by using the second non-interactive zero-knowledge proof to verify at least one factor of the payment confirmation data that is encrypted in the hash; and

write the payment confirmation data to the distributed ledger.

2. The system of claim 1, wherein the hashed memo comprises an encrypted version of data comprising a public key of the second entity, one or more transaction details, and the transaction confirmation identifier associated with the transaction.

3. The system of claim 1 or claim 2, wherein, when executed, the at least one application further causes the at least one of the plurality of nodes to at least:

receive, from the first entity, a non-interactive zero-knowledge proof for proving one or more factors associated with the authorization confirmation data without knowledge of the one or more factors; and

validate the authorization confirmation data based at least in part on the non-interactive zero-knowledge proof.

4. The system of any of claims 1 to 3, wherein the payment confirmation data comprises a hashed version of a transaction confirmation identifier associated with the transaction.

5. The system of any of claims 1 to 4, wherein, when executed, the at least one application further causes the at least one of the plurality of nodes to at least:

receive, from the second entity, a zero-knowledge proof for proving one or more factors associated with the payment confirmation data without knowledge of the one or more factors; and

validate the payment confirmation data based at least in part on the non-interactive zero-knowledge proof.

6. The system of any of claims 1 to 5, wherein, when executed, the at least one application further causes the at least one of the plurality of nodes to at least:

receive a request from the first entity to verify if the payment for the transaction has been processed;

confirm that the payment confirmation data is written on the distributed ledger; and

notify the first entity that the payment confirmation data is on the distributed ledger.

7. The system of any of claims 1 to 6, wherein the payment confirmation data is written to the distributed ledger according to a consensus agreement by the plurality of nodes.

8. The system of any of claims 1 to 7, wherein the authorization confirmation data is written to the distributed ledger according to a consensus agreement by the plurality of nodes.

9. A system, comprising:

at least one computing device associated with a first entity corresponding to a merchant;

at least one application executable by the at least one computing device, wherein, when executed, the at least one application causes the at least one computing device to at least:

transmit a transaction authorization request to a second entity corresponding to an issuer, the transaction authorization request being associated with a transaction between the first entity and the second entity;

receive an authorization for the transaction from the second entity, the authorization including a transaction confirmation identifier;

generate authorization confirmation data comprising a transaction authorization memo comprising the transaction confirmation identifier, transaction data associated with the transaction, and a public key associated with the second entity;

hash the transaction authorization memo to generate a hashed memo comprising an encrypted version of the authorization confirmation data; and

cause the hashed memo to be written to a distributed ledger by transmitting the hashed memo and a non-interactive zero-knowledge proof to a node of the distributed ledger, wherein the non-interactive zero-knowledge proof is provided to verify at least one factor of the authorization confirmation data that is encrypted in the hashed memo.

10. The system of claim 9, wherein the distributed ledger is hosted by a plurality of computing devices configured to store data according to a consensus agreement.

11. The system of claim 9 or claim 10, wherein, when executed, the at least one application further causes the at least one computing device to at least determine whether a payment associated with the transaction has been received from the second entity based at least in part on an inquiry into whether a payment transaction memo including the transaction confirmation identifier is recorded on the distributed ledger.

12. The system of claim 11, wherein, when executed, the at least one application further causes the at least one computing device to at least request the payment from the second entity in response to a determination that the payment transaction memo fails to exist on the distributed ledger.

13. The system of any of claims 9 to 12, wherein, when executed, the at least one application further causes the at least one computing device to at least sign the transaction authorization memo with a transmission private key of the first entity.

14. The system of claim 13, wherein causing the hashed transaction authorization memo to be written to the distributed ledger comprises transmitting, to at least one node of a plurality of nodes associated with the distributed ledger, the hashed authorization memo and a zero-knowledge proof for proving one or more factors associated with the transaction authorization memo without knowledge of the one or more factors.

15. The system of claim 14, wherein the transaction authorization memo is validated based at least in part on the non-interactive zero-knowledge proof.

16. A method, comprising:

receiving transaction authorization data and a non-interactive zero-knowledge proof from a first party of a transaction between the first party and a second party, the first party corresponding to a merchant system, the second party corresponding to an issuer system, wherein the transaction authorization data comprises a hashed memo comprising encrypted information that describes the transaction;

validating the transaction authorization data by using the non-interactive zero-knowledge proof to verify one or more factors of the transaction authorization data;

writing the transaction authorization data to a distributed ledger based at least in part on a consensus agreement;

receiving a payment confirmation request to determine if payment confirmation data associated with the transaction is recorded in the distributed ledger, the payment confirmation data corresponding to a hash of a transaction confirmation identifier for the transaction; and

determining whether the payment confirmation data is recorded in the distributed ledger.

17. The method of claim 16, wherein the encrypted information that describes the transaction comprises a hashed version of one or more transaction details associated with the transaction, a public key associated with the second party, and the transaction confirmation identifier that is unique to the transaction.

18. The method of claim 16 or claim 17,

wherein the zero-knowledge proof proves the one or more factors associated with the transaction authorization data without knowledge of the one or more factors.

19. The method of any of claims 16 to 18, further comprising:

receiving the payment confirmation data associated with the transaction from the second party; and

writing the payment confirmation data to the distributed ledger.

20. The method of claim 19, further comprising:

receiving, from the second party a second zero-knowledge proof for proving one or more factors associated with the payment confirmation data without knowledge of the one or more factors; and

validating the payment confirmation data using the non-interactive zero-knowledge proof.