

WHAT IS CLAIMED IS:

1. A computer-implemented method for privately verifying a sender, comprising:
receiving a transaction that identifies a transfer of an asset from the sender to a receiver,
wherein the transaction is signed by the sender with a one-time key that does not link
to a prior transaction of the sender;
privately sending, from the sender to the receiver, a public key identifying the sender;
generating at least one zero-knowledge proof that, when verified, proves that the one-
time key corresponds to the public key identifying the sender; and
writing the transaction and the at least one zero-knowledge proof to a public ledger,
wherein the transaction does not broadcast to the public ledger the identity of the
sender, and
wherein the receiver can verify the sender's identity by verifying the zero-knowledge
proof with the public key.
2. The computer-implemented method of claim 1, the privately sending further
comprising:
generating a shared key using an address associated with the receiver;
creating an encrypted public key using the shared key and the public key; and
including the encrypted public key in the transaction.
3. The computer-implemented method of claim 1, wherein the identity of the
receiver, the asset, and asset amount are encrypted on the public ledger and cannot be ascertained
from the public ledger by a third node.
4. The computer-implemented method of claim 1, wherein verifying the zero-
knowledge proof further validates the transfer on the public ledger by proving that the sender
owned the asset.
5. The computer-implemented method of claim 1, wherein the transaction further
comprises a unique nullifier that protects against a double-spend of the asset.

6. The computer-implemented system of claim 1, wherein the asset is a cryptocurrency.

7. The computer-implemented method of claim 1, wherein the public ledger is a blockchain.

8. The computer-implemented method of claim 1, the generating further comprising: generate the zero-knowledge proof using parallel processing.

9. A system for privately verifying a sender, comprising:
a memory; and

at least one processor coupled to the memory and configured to:

receive a transaction that identifies a transfer of an asset from the sender to a receiver, wherein the transaction is signed by the sender with a one-time key that does not link to a prior transaction of the sender;

privately send, from the sender to the receiver, a public key identifying the sender;
generate a zero-knowledge proof that, when verified, proves that the one-time key corresponds to the public key identifying the sender; and

write the transaction and the zero-knowledge proof to a public ledger, wherein the transaction does not broadcast to the public ledger the identity of the sender, and wherein the receiver can verify the sender's identity by verifying the zero-knowledge proof with the public key.

10. The system of claim 9, wherein to privately send the at least one processor is further configured to:

generate a shared key using an address associated with the receiver;
create an encrypted public key using the shared key and the public key; and
include the encrypted public key in the transaction.

11. The system of claim 9, wherein the identity of the receiver, the asset, and asset amount are encrypted on the public ledger and cannot be ascertained from the public ledger by a third node.
12. The system of claim 9, wherein verifying the zero-knowledge proof further validates the transfer on the public ledger by proving that the sender owned the asset.
13. The system of claim 9, wherein to generate the zero-knowledge proof the at least one processor is further configured to:
generate the zero-knowledge proof using parallel processing.
14. The system of claim 9, wherein the transaction further comprises a unique nullifier that protects against a double-spend of the asset.
15. The system of claim 9, wherein the asset is a cryptocurrency.
16. The system of claim 9, wherein the public ledger is a blockchain.
17. A non-transitory computer-readable device having instructions stored thereon that, when executed by at least one computing device, cause the at least one computing device to perform operations comprising:
receiving a transaction that identifies a transfer of an asset from the sender to a receiver, wherein the transaction is signed by the sender with a one-time key that does not link to a prior transaction of the sender;
privately sending, from the sender to the receiver, a public key identifying the sender;
generating a zero-knowledge proof that, when verified, proves that the one-time key corresponds to the public key identifying the sender; and
writing the transaction and the zero-knowledge proof to a public ledger, wherein the transaction does not broadcast to the public ledger the identity of the sender, and wherein the receiver can verify the sender's identity by verifying the zero-knowledge proof with the public key.

18. The non-transitory computer-readable device of claim 17, wherein verifying the zero-knowledge proof further validates the transfer on the public ledger by proving that the sender owned the asset.

19. The non-transitory computer-readable device of claim 17, wherein the identity of the receiver, the asset, and asset amount are encrypted on the public ledger and cannot be ascertained from the public ledger by a third node.

20. The non-transitory computer-readable device of claim 17, the operations further comprising:
generating the zero-knowledge proof using parallel processing.