CLAIMS

1. A system, comprising:

one or more memories; and

one or more processors coupled to the one or more memories and configured to:

generate an account private key associated with a new account;

derive a compute key associated with the new account from the account private key, wherein the compute key is configured to verify a new transaction to be confirmed on a blockchain, and wherein the new transaction is initiated by the new account, wherein the account private key cannot be recovered from the compute key;

receive, from the new account, a request to generate the new transaction, wherein the request includes a record associated with the new transaction;

generate the new transaction comprising to:

generate a signature based at least in part on the account private key and the record associated with the new transaction; and

cause a zero-knowledge proof to be generated using at least in part on the signature, an address associated with the new account, and the compute key; and

send the new transaction including the zero-knowledge proof to a verifier associated with the blockchain, wherein the zero-knowledge proof is configured to verify to the verifier that the signature associated with the new transaction belongs to the new account without revealing the signature to the verifier.

2. The system of claim 1, wherein the one or more processors are further configured to:

generate a view key associated with the new account based at least in part on the account private key, wherein the view key is configured to decrypt a portion of a confirmed transaction on the blockchain that belongs to the new account, wherein the account private key cannot be recovered from the view key; and

generate the address associated with the new account based at least in part on the view key, wherein the view key is configured to decrypt data encrypted by the address.

3. The system of claim 2, wherein the one or more processors are further configured to generate a graph key associated with the new account based at least in part on the view key, wherein the graph key is configured to generate a tag based at least in part on the new transaction, wherein the tag is included in the new transaction to mark the new transaction as being associated with the new account.

4. The system of claim 1, wherein the one or more processors are further configured to generate the account private key in response to a request to generate the new account.

5. The system of claim 1, wherein the record comprises zero or more input records and an output record, wherein the output record includes a recipient account address, wherein the one or more processors are further configured to:

encrypt the output record using the recipient account address, wherein the encrypted output record is decryptable using a recipient view key corresponding to the recipient account address.

6. The system of claim 5, wherein the zero or more input records each comprises the address associated with the new account, wherein the address is generated based at least in part on a view key that is derived from the account private key, wherein the account private key cannot be recovered from the view key.

7. The system of claim 5, wherein the zero or more input records comprise output record(s) of transactions previously confirmed on the blockchain.

8. The system of claim 5, wherein the one or more processors are further configured to:

generate a view key associated with the new account based at least in part on the account private key, wherein the view key is configured to decrypt a portion of a confirmed transaction on the blockchain that belongs to the new account, wherein the account private key cannot be recovered from the view key;

generate a graph key associated with the new account based at least in part on the view key;

generate a tag corresponding to the new transaction using at least one of the zero or more input records and the output record; and

prior to sending the new transaction to the verifier associated with the blockchain, include the tag in the new transaction.

9. The system of claim 1, wherein the one or more processors are further configured to:

generate a view key associated with the new account based at least in part on the account private key, wherein the view key is configured to decrypt a portion of a confirmed transaction on the blockchain that belongs to the new account, wherein the account private key cannot be recovered from the view key;

receive a request to determine whether the new account is a party to confirmed transaction(s) on the blockchain;

obtain new confirmed output records associated with the confirmed transaction(s);

determine a confirmed output record that can be decrypted using the view key, wherein the confirmed output record was encrypted using the address associated with the new account; and

present information on the confirmed output record at a user interface.

10. The system of claim 1, wherein the one or more processors are further configured to:

generate a view key associated with the new account based at least in part on the account private key, wherein the view key is configured to decrypt a portion of a confirmed transaction on the blockchain that belongs to the new account, wherein the account private key cannot be recovered from the view key;

generate a graph key associated with the new account based at least in part on the view key;

receive a request to track trends associated with the new account;

obtain confirmed transactions on the blockchain;

generate respective tags corresponding to the confirmed transactions using the graph key;

determine a subset of the confirmed transactions that includes a corresponding subset of the respective tags; and

analyze the subset of the confirmed transactions related to the new account for a trend or anomalous activity.

11. A method, comprising:

generating an account private key associated with a new account;

deriving a compute key associated with the new account from the account private key, wherein the compute key is configured to verify a new transaction to be confirmed on a blockchain, and wherein the new transaction is initiated by the new account, wherein the account private key cannot be recovered from the compute key;

receiving, from the new account, a request to generate the new transaction, wherein the request includes a record associated with the new transaction;

generating the new transaction comprises:

generating a signature based at least in part on the account private key and the record associated with the new transaction; and

causing a zero-knowledge proof to be generated using at least in part on the signature, an address associated with the new account, and the compute key; and

sending the new transaction including the zero-knowledge proof to a verifier associated with the blockchain, wherein the zero-knowledge proof is configured to verify to

the verifier that the signature associated with the new transaction belongs to the new account without revealing the signature to the verifier.

12. The method of claim 11, further comprising:

generating a view key associated with the new account based at least in part on the account private key, wherein the view key is configured to decrypt a portion of a confirmed transaction on the blockchain that belongs to the new account, wherein the account private key cannot be recovered from the view key; and

generating the address associated with the new account based at least in part on the view key, wherein the view key is configured to decrypt data encrypted by the address.

13. The method of claim 12, further comprising generating a graph key associated with the new account based at least in part on the view key, wherein the graph key is configured to generate a tag based at least in part on the new transaction, wherein the tag is included in the new transaction to mark the new transaction as being associated with the new account.

14. The method of claim 11, wherein the record comprises zero or more input records and an output record, wherein the output record includes a recipient account address, the method further comprising:

encrypting the output record using the recipient account address, wherein the encrypted output record is decryptable using a recipient view key corresponding to the recipient account address.

15. The method of claim 14, wherein the zero or more input records each comprises the address associated with the new account, wherein the address is generated based at least in part on a view key that is derived from the account private key, wherein the account private key cannot be recovered from the view key.

16. The method of claim 14, wherein the zero or more input records comprise output record(s) of transactions previously confirmed on the blockchain.

17. A computer program product comprising a non-transitory computer-readable storage medium and comprising having stored therein computer instructions that when executed by one or more processors, cause the one or more processors to perform operations comprising:

generating an account private key associated with a new account;

deriving a compute key associated with the new account from the account private key, wherein the compute key is configured to verify a new transaction to be confirmed on a blockchain, and wherein the new transaction is initiated by the new account, wherein the account private key cannot be recovered from the compute key;

receiving, from the new account, a request to generate the new transaction, wherein the request includes a record associated with the new transaction;

generating the new transaction comprises:

generating a signature based at least in part on the account private key and the record associated with the new transaction; and

causing a zero-knowledge proof to be generated using at least in part on the signature, an address associated with the new account, and the compute key; and

sending the new transaction including the zero-knowledge proof to a verifier associated with the blockchain, wherein the zero-knowledge proof is configured to verify to the verifier that the signature associated with the new transaction belongs to the new account without revealing the signature to the verifier.