THE INVENTION CLAIMED IS

1. A computer-implemented method for determining solvency of a digital asset exchange system, comprising:

   identifying, with at least one processor, a plurality of blockchain addresses corresponding to a plurality of users of the digital asset exchange system, each blockchain address of the plurality of blockchain addresses comprising a value generated by hashing a public key corresponding to a private key controlled by the digital asset exchange system, such that the public key and the private key are not exposed on a blockchain network;

   generating, with at least one processor, a first commitment to an amount of digital assets corresponding to the plurality of blockchain addresses;

   generating, with at least one processor, a second commitment to a balance of each user of the plurality of users;

   generating, with at least one processor, a first component of a zero-knowledge algorithm comprising a zkSNARK protocol that is configured to receive, as input, the first commitment, wherein the first component of the zero-knowledge algorithm proves to a verifying system that the digital asset exchange system knows all private keys used to generate the plurality of blockchain addresses;

   generating, with at least one processor, a second component of the zero-knowledge algorithm comprising a Sigma protocol that is configured to receive, as input, the second commitment, wherein the second component of the zero-knowledge algorithm proves to a verifying system that each user balance of the second commitment is included in the amount of digital assets, wherein the second component of the zero-knowledge algorithm further comprises a circuit configured to verify that each user balance has a value in an interval between zero and a maximum;

   and

   determining, with at least one processor, that the digital asset exchange system is solvent based on the zero-knowledge algorithm.

2. The computer-implemented method of claim 1, wherein the first component of the zero-knowledge algorithm is a Boolean function.

3. The computer-implemented method of claim 2, wherein the second component of the zero-knowledge algorithm is an algebraic function.

4. The computer-implemented method of claim 1, wherein the blockchain network comprises a Bitcoin public blockchain network.

5. The computer-implemented method of claim 1, wherein the first commitment comprises a first point along an elliptic curve, and wherein

the second commitment comprises a second point along an elliptic curve.

6. A system for determining solvency of a digital asset exchange system, comprising:

a secure data storage device comprising a plurality of public/private key pairs for a plurality of users of the digital asset exchange system; and

at least one processor in communication with a blockchain network, the at least one processor programmed or configured to:

identify a plurality of blockchain addresses corresponding to the plurality of users of the digital asset exchange system, each blockchain address of the plurality of blockchain addresses comprising a value generated by hashing a public key corresponding to a private key controlled by the digital asset exchange system and stored on the secure data storage device, such that the public key and the private key are not exposed on the blockchain network;

generate a first commitment to an amount of digital assets corresponding to the plurality of blockchain addresses;

generate a second commitment to a balance of each user of the plurality of users;

generate a first component of a zero-knowledge algorithm comprising a zkSNARK protocol that is configured to receive, as input, the first commitment, wherein the first component of the zero-knowledge algorithm proves to a verifying system that the digital asset exchange system knows all private keys used to generate the plurality of blockchain addresses;

generate a second component of the zero-knowledge algorithm comprising a Sigma protocol that is configured to receive, as input, the second commitment, wherein the second component of the zero-knowledge algorithm proves to a verifying system that each user balance of the second commitment is included in the amount of digital assets, wherein the second component of the zero-knowledge algorithm further comprises a circuit configured to verify that each user balance has a value in an interval between zero and a maximum; and

determine that the digital asset exchange system is solvent based on the zero-knowledge algorithm.

7. The system of claim 6, wherein the first component of the zero-knowledge algorithm is a Boolean function.

8. The system of claim 7, wherein the second component of the zero-knowledge algorithm is an algebraic function.

9. The system of claim 6, wherein the blockchain network comprises a Bitcoin public blockchain network.

10. The system of claim 6, wherein the first commitment comprises a first point along an elliptic curve, and wherein the second commitment comprises a second point along an elliptic curve.

11. A computer program product for determining solvency of a digital asset exchange system, comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, cause the at least one processor to:

identify a plurality of blockchain addresses of a blockchain network corresponding to a plurality of users of the digital asset exchange system, each blockchain address of the plurality of blockchain addresses comprising a value generated by hashing a public key corresponding to a private key controlled by the digital asset exchange system and stored on the secure data storage device, such that the public key and the private key are not exposed on a blockchain network;

generate a first commitment to an amount of digital assets corresponding to the plurality of blockchain addresses;

generate a second commitment to a balance of each user of the plurality of users;

generate a first component of a zero-knowledge algorithm comprising a zkSNARK protocol that is configured to receive, as input, the first commitment, wherein the first component of the zero-knowledge algorithm proves to a verifying system that the digital asset exchange system knows all private keys used to generate the plurality of blockchain addresses;

generate a second component of the zero-knowledge algorithm comprising a Sigma protocol that is configured to receive, as input, the second commitment, wherein the second component of the zero-knowledge algorithm proves to a verifying system that each user balance of the second commitment is included in the amount of digital assets, wherein the second component of the zero-knowledge algorithm further comprises a circuit configured to verify that each user balance has a value in an interval between zero and a maximum; and

determine that the digital asset exchange system is solvent based on the zero-knowledge algorithm.

12. The computer program product of claim 11, wherein the first component of the zero-knowledge algorithm is a Boolean function.

13. The computer program product of claim 12, wherein the second component of the zero-knowledge algorithm is an algebraic function.

14. The computer program product of claim 11, wherein the blockchain network comprises a Bitcoin public blockchain network.