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 configured to receive, as input, the first commitment, and to output a value generated based on each public key corresponding to each blockchain address, such that the first component of the zero-knowledge algorithm proves to a verifying system that the digital asset exchange system has access to each public key corresponding to each blockchain address;

generating, with at least one processor, a second component of the zero-knowledge algorithm configured to receive, as input, the second commitment, and to output a value generated based on each user balance, such that the second component of the zero-knowledge algorithm proves to a verifying system that each user balance is included in the amount of digital assets; 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 comprises a zkSNARK protocol, and wherein the second component of the zero-knowledge algorithm comprises a Sigma protocol.

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

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

5. The computer-implemented method of claim 4, wherein determining that the digital asset exchange system is solvent comprises determining if an output of the algebraic function is an input to the Boolean function.

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

7. 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.

8. 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 configured to receive, as input, the first commitment, and to output a value generated based on each public key corresponding to each blockchain address, such that the first component of the zero-knowledge algorithm proves to a verifying system that the digital asset exchange system has access to each public key corresponding to each blockchain address;

generate a second component of the zero-knowledge algorithm configured to receive, as input, the second commitment, and to output a value generated based on each user balance, such that the second component of the zero-knowledge algorithm proves to a verifying system that each user balance is included in the amount of digital assets; and

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

9. The system of claim 8, wherein the first component of the zero-knowledge algorithm comprises a zkSNARK protocol, and wherein the second component of the zero-knowledge algorithm comprises a Sigma protocol.

10. The system of claim 8, wherein the first component of the zero-knowledge algorithm is a Boolean function.

11. The system of claim 10, wherein the second component of the zero-knowledge algorithm is an algebraic function.

12. The system of claim 11, wherein determining that the digital asset exchange system is solvent comprises determining if an output of the algebraic function is an input to the Boolean function.

13. The system of claim 8, wherein the blockchain network comprises the Bitcoin public blockchain network.

14. The system of claim 8, 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.

15. 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 configured to receive, as input, the first commitment, and to output a value generated based on each public key corresponding to each blockchain address, such that the first component of the zero-knowledge algorithm proves to a verifying system that the digital asset exchange system has access to each public key corresponding to each blockchain address;

generate a second component of the zero-knowledge algorithm configured to receive, as input, the second commitment, and to output a value generated based on each user balance, such that the second component of the zero-knowledge algorithm proves to a verifying system that each user balance is included in the amount of digital assets; and

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

16. The computer program product of claim 15, wherein the first component of the zero-knowledge algorithm comprises a zkSNARK protocol, and wherein the second component of the zero-knowledge algorithm comprises a Sigma protocol.

17. The computer program product of claim 15, wherein the first component of the zero-knowledge algorithm is a Boolean function.

18. The computer program product of claim 17, wherein the second component of the zero-knowledge algorithm is an algebraic function.

19. The computer program product of claim 18, wherein determining that the digital asset exchange system is solvent comprises determining if an output of the algebraic function is an input to the Boolean function.

20. The computer program product of claim 15, wherein the blockchain network comprises the Bitcoin public blockchain network.

21. The computer program product of claim 15, 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.

22. A computer-implemented method for generating and verifying anonymous digital certificates, comprising:

generating, with at least one processor of a proving system, a digital signature by encrypting a hashed message with a private key based on an asymmetrical encryption algorithm;

communicating, with the at least one processor, the digital signature to a verifying system;

generating, with the at least one processor, a commitment to a message used to generate the hashed message;

generating, with the at least one processor, a first component of a zero-knowledge algorithm configured to receive, as input, the commitment, and output a value based on the message used to generate the hashed message;

generating, with the at least one processor, a second component of the zero-knowledge algorithm configured to receive, as input, the commitment, and output a value based on the private key used to generate the digital signature; and

generating, with the at least one processor, the zero-knowledge algorithm based on the first component and the second component.

23. The computer-implemented method of claim 22, wherein the commitment to the message comprises a point along an elliptic curve.

24. The computer-implemented method of claim 22, further comprising verifying, by at least one processor of the verifying system, the digital signature based on the commitment and the zero-knowledge algorithm.

25. The computer-implemented method of claim 22, wherein the first component of the zero-knowledge algorithm comprises a zkSNARK protocol, and wherein the second component of the zero-knowledge algorithm comprises a Sigma protocol.

26. The computer-implemented method of claim 22, wherein the first component of the zero-knowledge algorithm is a Boolean function.

27. The computer-implemented method of claim 25, wherein the second component of the zero-knowledge algorithm is an algebraic function.

28. The computer-implemented method of claim 27, further comprising verifying the digital signature based on the zero-knowledge algorithm by determining that an output of the algebraic function is an input to the Boolean function.

29. A system for generating and verifying anonymous digital certificates, comprising:

a secure data storage device comprising a private key of a public/private key pair and a message; and

a proving computer comprising at least one processor programmed or configured to:

generate a digital signature by encrypting a hash of the message with the private key based on an asymmetrical encryption algorithm;

communicate the digital signature to a verifying computer;

generate a commitment to the message;

generate a first component of a zero-knowledge algorithm configured to receive, as input, the commitment, and output a value based on the message used to generate the hashed message;

generate a second component of the zero-knowledge algorithm configured to receive, as input, the commitment, and output a value based on the private key used to generate the digital signature;

generate the zero-knowledge algorithm based on the first component and the second component; and

communicate the zero-knowledge algorithm to the verifying computer.

30. The system of claim 29, wherein the commitment to the message comprises a point along an elliptic curve.

31. The system of claim 29, further comprising the verifying computer, the verifying computer including at least one processor programmed or configured to verify the digital signature based on the commitment and the zero-knowledge algorithm.

32. The system of claim 29, wherein the first component of the zero-knowledge algorithm comprises a zkSNARK protocol, and wherein the second component of the zero-knowledge algorithm comprises a Sigma protocol.

33. The system of claim 29, wherein the first component of the zero-knowledge algorithm is a Boolean function.

34. The system of claim 33, wherein the second component of the zero-knowledge algorithm is an algebraic function.

35. The system of claim 34, further comprising verifying the digital signature based on the zero-knowledge algorithm by determining that an output of the algebraic function is an input to the Boolean function.

36. A computer program product for generating and verifying anonymous digital certificates, 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:

generate a digital signature by encrypting a hash of the message with a private key based on an asymmetrical encryption algorithm;

communicate the digital signature to a verifying computer;

generate a commitment to the message;

generate a first component of a zero-knowledge algorithm configured to receive, as input, the commitment, and output a value based on the message used to generate the hashed message;

generate a second component of the zero-knowledge algorithm configured to receive, as input, the commitment, and output a value based on the private key used to generate the digital signature;

generate the zero-knowledge algorithm based on the first component and the second component; and

communicate the zero-knowledge algorithm to the verifying computer.

37. The computer program product of claim 36, wherein the commitment to the message comprises a point along an elliptic curve.

38. The computer program product of claim 36, wherein the first component of the zero-knowledge algorithm comprises a zkSNARK protocol, and wherein the second component of the zero-knowledge algorithm comprises a Sigma protocol.

39. The computer program product of claim 36, wherein the first component of the zero-knowledge algorithm is a Boolean function.

40. The computer program product of claim 39, wherein the second component of the zero-knowledge algorithm is an algebraic function.

~~41. The computer program product of claim 40, further comprising verifying the digital signature based on the zero-knowledge algorithm by determining that an output of the algebraic function is an input to the Boolean function.~~

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.