

CLAIMS

What is claimed is:

1. A computer-implemented method comprising:
receiving, by a central entity computer, a request for digital currency, the request comprising a serial number and a denomination of a physical currency;
generating, by the central entity computer, the digital currency for the denomination and linked to the serial number, wherein the generating comprises recording the digital currency on a blockchain;
transmitting, by the central entity computer, a notification of the generation of the digital currency; and
causing, by the central entity computer, removal of the physical currency from circulation in a fiat currency system.
2. The method of claim 1, further comprising:
associating the digital currency with a digital wallet using a private key stored to the digital wallet.
3. The method of claim 2, wherein the private key of the digital wallet is stored on a chip of a smart card or a secure element of a user device.
4. The method of claim 1, further comprising:
receiving, by the central entity computer from a transaction processing network, a trusted certificate for the central entity computer; and
using the trusted certificate to generate the digital currency.
5. The method of claim 1, wherein, prior to transmitting the notification of the generation of the digital currency, the recording of the digital currency on the blockchain is validated by a plurality of validating entities.
6. The method of claim 1, wherein the digital currency is recorded on the blockchain using a public key of the central entity computer.

7. The method of claim 1, wherein causing the removal of the physical currency from circulation includes physically destroying the physical currency, the physical currency being fiat currency.

8. The method claim 1, wherein the request for digital currency is a first request and the physical currency is a first physical currency, the method further comprising:

receiving, by the central entity computer, a second request for digital currency, the second request comprising a serial number and a denomination of a second physical currency, wherein the serial number and the denomination of the second physical currency are the same as the serial number and the denomination of the first physical currency;

determining, by the central entity computer, that the digital currency corresponding to the serial number and denomination is already recorded on the blockchain; and

refraining from generating a second digital currency based on the second request.

9. The method of claim 1, wherein the blockchain includes a plurality of blocks, at least one block, of the plurality of blocks, storing data for a plurality of transactions, the plurality of transactions including a first record indicating that the digital currency for an amount associated with the denomination has been created, the first record including a public key associated with a digital wallet.

10. The method of claim 1, wherein the blockchain includes a plurality of blocks, at least one block, of the plurality of blocks, storing data for a plurality of transactions, the plurality of transactions including a second record recording the removal of the physical currency from circulation.

11. A central entity computer comprising:
a processor; and
a non-transitory computer-readable medium comprising code, executable by the processor, for implementing a method comprising:

receiving, by the central entity computer, a request for digital currency, the request comprising a serial number and a denomination of a physical currency;

generating, by the central entity computer, the digital currency for the denomination and linked to the serial number, wherein the generating comprises recording the digital currency on a blockchain;

transmitting, by the central entity computer, a notification of the generation of the digital currency; and

causing, by the central entity computer, removal of the physical currency from circulation in a fiat currency system.

12. The central entity computer of claim 11, further comprising:

associating the digital currency with a first digital wallet using a private key stored to the first digital wallet, wherein the private key of the first digital wallet is stored on a chip of a smart card or a secure element of a user device.

13. The central entity computer of claim 11, the method further comprising:

receiving, by the central entity computer from a transaction processing network, a trusted certificate for the central entity computer; and

using the trusted certificate to generate the digital currency.

14. The central entity computer of claim 11, wherein, prior to transmitting the notification of the generation of the digital currency, the recording of the digital currency on the blockchain is validated by a plurality of validating entities.

15. The central entity computer of claim 11, wherein the digital currency is recorded on the blockchain using a public key of the central entity computer.

16. The central entity computer of claim 11, wherein recording the digital currency on the blockchain generates a record in a block in the blockchain, the record comprising a currency type of the physical currency and the serial number of the physical currency.

17. The central entity computer of claim 11, wherein causing the removal of the physical currency from circulation includes physically destroying the physical currency, the physical currency being fiat currency.

18. The central entity computer of claim 11, wherein the request for digital currency is a first request and the physical currency is a first physical currency, the method further comprising:

receiving, by the central entity computer, a second request for digital currency, the second request comprising a serial number and a denomination of a second physical currency, wherein the serial number and the denomination of the second physical currency are the same as the serial number and the denomination of the first physical currency;

determining, by the central entity computer, that the digital currency corresponding to the serial number and denomination is already recorded on the blockchain; and

refraining from generating a second digital currency based on the second request.

19. The central entity computer of claim 11, wherein the blockchain includes a plurality of blocks, at least one block, of the plurality of blocks, storing data for a plurality of transactions, the plurality of transactions including a first record indicating that the digital currency for an amount associated with the denomination has been created, the first record including a public key associated with a digital wallet.

20. The central entity computer of claim 11, wherein the blockchain includes a plurality of blocks, at least one block, of the plurality of blocks, storing data for a plurality of transactions, the plurality of transactions including a second record recording the removal of the physical currency from circulation.

21. A computer-implemented method comprising:

receiving, by a blockchain node storing a blockchain, a request to record an action relating to removal of physical currency with a denomination from a fiat currency system;

recording, by the blockchain node, a record of the action relating to the removal of the physical currency with the denomination from the fiat currency system to the blockchain;

receiving, by the blockchain node, a request to record digital currency in an amount equal to the denomination, the digital currency associated with a public key of a user; and

recording, by the blockchain node, the digital currency in an amount equal to the denomination.

22. The method of claim 21, further comprising:

receiving, by the blockchain node, a request to record a transaction between a first user and a second user, the request including a public key of the first user, a public key of the second user, and a transaction amount; and

recording a record of the transaction between the first user and the second user, the record of the transaction including a public key of the first user, a public key of the second user, and the transaction amount in a block along with the action relating to removal of physical currency with a denomination from the fiat currency system to the blockchain.

23. The method of claim 22, the record further comprising a currency type of the physical currency.

24. The method of claim 21, wherein the digital currency in the amount equal to the denomination is recorded to a record, the record further comprising a currency type of the physical currency and a serial number of the physical currency.

25. The method of claim 21, wherein the blockchain node is a bank server computer.

26. The method of claim 21, wherein the request is signed using a private key of the first user.

27. The method of claim 26, further comprising validating a digital signature of the first user using the public key of the first user.

28. The method of claim 21, further comprising reaching consensus with a plurality of additional blockchain nodes.

29. The method of claim 28, wherein the consensus is reached using one of: proof of stake, a byzantine fault tolerant algorithm, or a crash-fault tolerant algorithm.

30. The method of claim 21, wherein the blockchain node uses a certificate to gain permission to write to the blockchain.

31. A central entity computer comprising:
a processor; and
a non-transitory computer-readable medium comprising code, executable by the processor, for implementing a method comprising:
receiving, by a blockchain node storing a blockchain, a request to record an action relating to removal of physical currency with a denomination from a fiat currency system;
recording, by the blockchain node, a record of the action relating to the removal of the physical currency with the denomination from the fiat currency system to the blockchain;
receiving, by the blockchain node, a request to record digital currency in an amount equal to the denomination, the digital currency associated with a public key of a user; and
recording, by the blockchain node, the digital currency in an amount equal to the denomination.

32. The central entity computer of claim 31, the method further comprising:

receiving, by the blockchain node, a request to record a transaction between a first user and a second user, the request including a public key of the first user, a public key of the second user, and a transaction amount; and

recording a record of the transaction between the first user and the second user, the record of the transaction including a public key of the first user, a public key of the second user, and the transaction amount in a block along with the action relating to removal of physical currency with a denomination from the fiat currency system to the blockchain.

33. The central entity computer of claim 32, the record further comprising a currency type of the physical currency.

34. The central entity computer of claim 31, wherein the digital currency in the amount equal to the denomination is recorded to a record, the record further comprising a currency type of the physical currency and a serial number of the physical currency.

35. The central entity computer of claim 31, wherein the blockchain node is a bank server computer.

36. The central entity computer of claim 31, wherein the request is signed using a private key of the first user.

37. The central entity computer of claim 36, the method further comprising validating a digital signature of the first user using the public key of the first user.

38. The central entity computer of claim 31, further comprising reaching consensus with a plurality of additional blockchain nodes.

39. The central entity computer of claim 38, wherein the consensus is reached using one of: proof of stake, a byzantine fault tolerant algorithm, or a crash-fault tolerant algorithm.

40. The central entity computer of claim 31, wherein the blockchain node uses a certificate to gain permission to write to the blockchain.