

CLAIMS

What is claimed is:

1. A computer-implemented method comprising:

receiving, by a central entity computer from a transaction processing network, a trusted certificate that grants permission to the central entity computer to generate or destroy digital currency, wherein the central entity computer is associated with a central bank;

receiving, by ~~the a~~ central entity computer from a redeeming entity device associated with a bank granted permission by the transaction processing network to validate transactions, a request for digital currency, the request comprising a serial number and a denomination of a physical currency;

generating, by the central entity computer using the trusted certificate, the digital currency for the denomination and linked to the serial number, wherein the generating comprises recording the digital currency on a blockchain to a record that includes the serial number of the physical currency;

transmitting, by the central entity computer to the redeeming entity device, a notification of ~~the~~ generation of the digital currency, 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; 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 any one of claims 1—3, 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.~~

54. The method of any one of claims 1 – 43, wherein the digital currency is recorded on the blockchain using a public key of the central entity computer.

65. A computer-implemented method comprising:
receiving, by a central entity computer from a transaction processing network, a trusted certificate that grants permission to the central entity computer to generate or destroy digital currency, wherein the central entity computer is associated with a central bank;

receiving, by the a-central entity computer from a redeeming entity device associated with a bank granted permission by the transaction processing network to validate transactions, a request for digital currency, the request comprising a serial number and a denomination of a physical currency;

generating, by the central entity computer using the trusted certificate, the digital currency for the denomination and linked to the serial number, wherein the generating comprises recording the digital currency on a blockchain to a record that includes the serial number of the physical currency;

transmitting, by the central entity computer to the redeeming entity device, 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, wherein causing the removal of the physical currency from the circulation includes physically destroying the physical currency, the physical currency being fiat currency.

76. A computer-implemented method comprising:

receiving, by a central entity computer from a transaction processing network, a trusted certificate that grants permission to the central entity computer to generate or destroy digital currency, wherein the central entity computer is associated with a central bank;

receiving, by the a central entity computer from a redeeming entity device associated with a bank granted permission by the transaction processing network to validate transactions, a request for digital currency, the request comprising a serial number and a denomination of a physical currency;

generating, by the central entity computer using the trusted certificate, the digital currency for the denomination and linked to the serial number, wherein the generating comprises recording the digital currency on a blockchain to a record that includes the serial number of the physical currency;

transmitting, by the central entity computer to the redeeming entity device, a notification of ~~the~~ generation of the digital currency;

causing, by the central entity computer, removal of the physical currency from circulation in a fiat currency system, wherein the request for digital currency is a first request and the physical currency is a first physical currency;

receiving, by the central entity computer from the redeeming entity device associated with a bank granted permission by the transaction processing network to validate transactions, 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 the denomination is already recorded on the blockchain; and

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

87. The method of any one of claims 1—3, 5, or 76, 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 (or the digital wallet when dependent on claim 3).

98. A computer-implemented method comprising:

receiving, by a central entity computer from a transaction processing network, a trusted certificate that grants permission to the central entity computer to generate or destroy digital currency, wherein the central entity computer is associated with a central bank;

receiving, by the central entity computer from a redeeming entity device associated with a bank granted permission by the transaction processing network to validate transactions, a request for digital currency, the request comprising a serial number and a denomination of a physical currency;

generating, by the central entity computer using the trusted certificate, the digital currency for the denomination and linked to the serial number, wherein the generating comprises recording the digital currency on a blockchain to a record that includes the serial number of the physical currency;

transmitting, by the central entity computer to the redeeming entity device, 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, 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 the circulation.

~~109.~~ A central entity computer comprising:

a processor; and

a non-transitory computer-readable medium comprising code, executable by the processor, for implementing a method as recited in any one of claims 1 – 98.

~~11~~10. A computer-implemented method comprising:

receiving, by a blockchain node storing in 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, the record indicating that a particular unit of the physical currency has been removed from circulation;

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

recording, by the blockchain node, the digital currency in ~~thea~~ amount equal to the denomination, wherein the digital currency and the record of the removal are validated by a plurality of blockchain nodes using proof of stake consensus.

~~12~~11. The method of claim ~~11~~10, 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 ~~thea~~ public key of the first user, ~~thea~~ 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.

~~13~~12. The method of claim ~~12~~11, the record further comprising a currency type of the physical currency.

~~14~~13. The method of any one of claims ~~11~~10 – ~~13~~12, 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.

~~15~~14. The method of any one of claims ~~11~~10 – ~~14~~13, wherein the blockchain node is a bank server computer.

~~16~~15. The method of any one of claims ~~11~~10 – ~~15~~14, wherein the request is signed using a private key of the user.

~~17~~16. The method of claim ~~16~~15, further comprising validating a digital signature of the user using the public key of the user.

~~18. The method of any one of claims 11 – 17, further comprising reaching consensus with a plurality of additional blockchain nodes, wherein the consensus is reached using one of: proof of stake, a byzantine fault tolerant algorithm, or a crash fault tolerant algorithm.~~

1917. The method of any one of claims ~~11~~10 – ~~18~~16, wherein the blockchain node uses a certificate to gain permission to write to the blockchain.

~~20~~18. A computing device comprising:
a processor; and
a non-transitory computer-readable medium comprising code,
executable by the processor, for implementing a method as recited in any one of
claims ~~11~~10 – ~~19~~17.