

WHAT IS CLAIMED IS:

1. A method comprising:

accessing, with a computer system for respective first and second internal user accounts of
5 a transaction service provided by the computer system, first and second cryptographic key pairs,
wherein the first and second cryptographic key pairs are useable to authenticate transactions for
recording on a blockchain;

storing, at the computer system, private keys of the first and second cryptographic key pairs
such that owners of the first and second internal user accounts cannot access the private keys;

10 receiving, at the computer system, an indication of a first incoming transaction transferring
a first digital asset from outside the transaction service to the first internal user account, wherein
the first incoming transaction is recorded on the blockchain, wherein the indication of the first
incoming transaction includes an indication of a public key of the first cryptographic key pair; and

in response to a request from the first internal user account, transferring, by the computer
15 system in a first internal transaction, ownership of a portion of the first digital asset from the first
internal user account to the second internal user account without performing a cryptographic
operation using the private key of the first cryptographic key pair to cause recording of the
transfer on the blockchain, wherein the transferring is recorded using an internal ledger of the
transaction service.

20 2. The method of claim 1, wherein the request from the owner of the first internal user account
includes a non-cryptographic account indicator of the second internal user account.

3. The method of claim 1, further comprising

25 performing, with the computer system using the internal ledger, an outgoing transaction
transferring one or more digital assets to a recipient external user account from an internal user
account, wherein the computer system performs a cryptographic operation using a private key of
a cryptographic key pair to cause recording of the outgoing transaction on the blockchain.

30 4. The method of claim 1, further comprising:

in response to a request from the second internal user account, sending, by the computer
system using the internal ledger and the private key of the first cryptographic key pair, an indicator
of an outgoing transaction transferring ownership of one or more digital assets from the second
internal user account to a recipient external user account that is outside of the transaction service;

wherein the indicator causes the outgoing transaction to be recorded on the blockchain as an indicator of the first internal user account transferring the portion of the first digital asset directly to an indicator of the recipient external user account.

5 5. The method of claim 4, further comprising:

receiving, at the computer system, an indication of a second incoming transaction transferring a second digital asset from outside the transaction service to the second internal user account, wherein the second incoming transaction is recorded on the blockchain, wherein the indication of the second incoming transaction includes an indication of a public key of the second
10 cryptographic key pair; and

wherein the computer system also uses the private key of the second cryptographic key pair while sending the indicator of the outgoing transaction; and

wherein the indicator causes the outgoing transaction to be recorded on the blockchain as:

(a) the indicator of the first internal user account transferring the portion of the first
15 digital asset directly to the indicator of the recipient external user account, and

(b) an indicator of the second internal user account transferring a portion of the second digital asset to the indicator of the recipient external user account.

6. The method of claim 1,

20 wherein subsequent to the first internal transaction, the blockchain indicates that the portion of the first digital asset is still assigned to the first internal user account;

the method further comprising:

causing, by the computer system and based on the blockchain and the internal ledger, a user interface to be presented to the owner of the first internal user account indicating that the
25 portion of the first digital asset is not assigned to the first internal user account.

7. The method of claim 1, further comprising:

recording, with the computer system in the internal ledger and not on the blockchain, a plurality of subsequent internal transactions transferring digital assets between a set of internal
30 user accounts of the transaction service including the first internal user account and the second internal user account; and

sending, by the computer system using the internal ledger and a private key of a cryptographic key pair of a particular internal user account of the set of internal user accounts, an indicator of an outgoing transaction transferring ownership of one or more digital assets from the

particular internal user account and to a recipient external user account that is outside of the transaction service, wherein the outgoing transaction is recorded to the blockchain by adding two blocks to the blockchain.

- 5 8. The method of claim 7,
 wherein the two blocks include:
 a first block indicative of a transfer of one or more digital assets to the particular
 internal user account from a first subset of the set of internal user accounts; and
 a second block indicative of a transfer of one or more digital assets to the recipient
10 external user account from a second subset of the set of internal user accounts.
9. The method of claim 7, further comprising:
 wherein the subsequent internal transactions do not include a transaction transferring
 digital assets from the second internal user account to the first internal user account; and
15 wherein the two blocks include a first block indicative of a transfer of digital assets from
 the second internal user account to the first internal user account.
10. A non-transitory, computer-readable medium storing instructions that when executed by a
computer system cause the computer system to perform operations comprising:
20 accessing, for respective ones of a plurality of internal user accounts of a transaction
service, a plurality of respective cryptographic key pairs, wherein the cryptographic key pairs are
useable to authenticate transactions for recordation on a blockchain;
 storing private keys of the cryptographic key pairs such that owners of the internal user
accounts cannot access the private keys;
25 receiving indications of a plurality of incoming transactions transferring respective digital
assets from respective source external user accounts outside the transaction service to respective
internal user accounts, wherein the incoming transactions are recorded on the blockchain, wherein
the indications of the plurality of incoming transactions include indications of one or more public
keys of the cryptographic key pairs; and
30 in response to respective requests from respective ones of the internal user accounts,
transferring, in respective internal transactions, ownership of digital assets between pairs of
internal user accounts, wherein the internal transactions are not recorded on the blockchain and
wherein indications of the internal transactions are recorded with an internal ledger of the
transaction service.

11. The non-transitory, computer-readable medium of claim 10, wherein incoming transactions to the transaction service and outgoing transactions from the transaction service are initiated using cryptographic identifiers whereas the internal transactions within the transaction service are initiated using non-cryptographic account indicators of the internal user accounts.

12. The non-transitory, computer-readable medium of claim 10, wherein a first internal transaction of the internal transactions transferred one or more digital assets from a first internal user account to a second internal user account;

wherein the operations further include:

in response to a request from the second internal user account, sending using the internal ledger and the private key of the cryptographic key pair corresponding to the first internal user account, an indicator of an outgoing transaction transferring one or more digital assets to a recipient external user account from the first internal user account, wherein the outgoing transaction is recorded on the blockchain using one or more blocks.

13. The non-transitory, computer-readable medium of claim 12, wherein one of the one or more blocks indicates a transfer from the second internal user account to the recipient external user account.

14. The non-transitory, computer-readable medium of claim 12, wherein one of the one or more blocks indicates a transfer from the first internal user account to the second internal user account.

15. The non-transitory, computer-readable medium of claim 10, wherein the operations further include:

causing user interfaces to be presented to the owners of the internal user accounts, wherein a given user interface presents information about the digital assets assigned to a given internal user account, wherein the information is based on the blockchain and the internal ledger.

16. The non-transitory, computer-readable medium of claim 15, wherein when the blockchain indicates that a particular digital asset is assigned to a first internal user account but the internal ledger indicates that the particular digital asset is assigned to a second internal user account:

the user interface presented to the owner of the first internal user account indicates that the particular digital asset is not assigned to the first internal user account, and
the user interface presented to the owner of the second internal user account indicates that the particular digital asset is assigned to the second internal user account.

5

17. — A method comprising:

receiving, at a computer system providing a transaction service, indications of a plurality of incoming transactions transferring respective digital assets from respective source external user accounts outside the transaction service to respective internal user accounts, wherein the incoming transactions are recorded on a blockchain, wherein the indications of the plurality of incoming transactions include indications of one or more public keys of cryptographic key pairs corresponding to respective internal user accounts of the transaction service;

10

in response to respective requests from respective ones of the internal user accounts, transferring, with the computer system between pairs of internal user accounts in respective internal transactions, ownership of digital assets between the pairs of internal user accounts, wherein the internal transactions are not recorded on the blockchain and wherein indications of the internal transactions are recorded with an internal ledger of the transaction service; and

15

in response to a request from a particular internal user account, performing, with the computer system using the internal ledger, an outgoing transaction transferring one or more digital assets to a recipient external user account from one or more internal user accounts, wherein the outgoing transaction is recorded on the blockchain;

20

wherein owners of respective ones of the internal user accounts are only able to access the internal user accounts through the transaction service.

25

18. — The method of claim 17,

wherein a first internal transaction of internal transactions transferred one or more digital assets from a different internal user account to the particular internal user account;

wherein the outgoing transaction is performed using a private key of a cryptographic key pair corresponding to the different internal user account; and

30

wherein the outgoing transaction is recorded on the blockchain by a block that is indicative of the different internal user account transferring one or more digital assets to the recipient external user account.

19. — The method of claim 17, wherein the digital assets are cryptocurrency.

20. ~~The method of claim 19,~~

~~wherein as a result of the incoming transactions, balances of cryptocurrency corresponding to the internal user accounts are in a first state;~~

5 ~~wherein as a result of the internal transactions, balances of cryptocurrency corresponding to the internal user accounts are in a different, second state according to the internal ledger but remain in the first state according to the blockchain; and~~

~~wherein as a result of the outgoing transaction, balances of cryptocurrency corresponding to at least some of the internal user accounts as indicated by the blockchain are updated to the~~
10 ~~second state by causing one or more blocks to be added to the blockchain.~~