

Claims

1. A computer-implemented method for performing a transfer of at least one resource across a network from a user's non-custodial wallet to a recipient, comprising the steps:
5 receiving a first share (C) of a private key from a first network entity (5) by a second network entity (3) which has access to a second share (A) of the private key;
 using the first and second shares (C, A) to generate a private key;
 creating, at the second network entity, a blockchain transaction (TX_i) for performing the transfer from the user's wallet (4) to the recipient (2) based on transfer-related
10 data and signed using the private key;
 and
 submitting the transaction to a blockchain network (7).
2. A method according to claim 1, and further comprising the step:
15 using the first network entity (5), to:
 receive a digital signature associated with the user (1) and transfer-related data; and
 verify the digital signature;
 and
 if verification is successful, providing the first share (C) of the private key to the second
20 network entity (3).
3. A method according to claim 1 or 2, and further comprising the step of:
 storing a third share (B) of the private key at, on or in association with, the user's wallet.
- 25 4. A method according to claim 1, 2 or 3, and further comprising the step of:
 splitting the private key into a plurality of shares and distributing at least one share to at least one of the user's wallet (4), the first network entity (5) and/or the second network entity (3).
- 30 5. A method according to any preceding claim, and further comprising the step of:
 in response to a security device being presented at a recipient device, generating a transfer request which requests the transfer from a user's non-custodial wallet to a recipient and includes the transfer-related data;
 sending the transfer request from the recipient device to a third network entity (8).

6. A method according to claim 5 and further comprising the step of:
receiving the transfer request at the third network entity;
generating an authorisation message comprising at least the digital signature
associated with the user and the transfer-related data, and providing the authorisation
to the first network entity.
7. A method according to any preceding claim, wherein:
the security device is or comprises: a smart card, a payment card, a hardware token,
a biometric data reader, a wireless or contactless data component such as Bluetooth
or NFC, one or more hardware and/or software components for facilitating verification
of a user's identity; and/or
the recipient device is or comprises an electronic point-of-sale (PoS) device, a terminal,
laptop, mobile device and/or processor-based device; and/or
the first network entity is a security device provider (5); and/or
the second network entity is a wallet provider (3); and/or
the third network entity is an acquirer (8).
8. A method according to any preceding claim, wherein the transfer related data
comprises one or more of: a currency indicator, a value or quantity relating to the
resource and/or data relating to an account or a security device associated with the
user.
9. A method according to any preceding claim, and further comprising the step of:
determining whether or not that the user's non-custodial wallet is able to complete the
transfer of the resource to the recipient.
10. A method according to claim 9 and further comprising the step of:
sending a transfer authorisation message from the second network entity to the first
network entity and/or recipient device if it is determined that the user's non-custodial
wallet is able to complete the transfer of the resource to the recipient;
or
sending a transfer decline message from the second network entity to the first network
entity, third network entity and/or recipient device if it is determined that the user's non-
custodial wallet is not able to complete the transfer of the resource to the recipient.

11. A method according to any preceding claim, wherein:
the step of using the first and second shares (C, A) to generate a private key is performed by the second network entity.
- 5 12. A method according to any preceding claim, wherein:
the blockchain transaction (TX_i) comprises an output arranged to perform the transfer of the at least one resource from the user's wallet to the recipient, and wherein the resource is or comprises a portion of cryptocurrency.
- 10 13. A method according to any preceding claim, and further comprising the step of:
converting a portion of a first currency to a portion of a second currency and providing the portion of the second currency to the first network entity.
14. A method according to any preceding claim, and further comprising the step of:
15 transferring the resource from the first network entity to the recipient.
15. A method according to any preceding claim, wherein the user's non-custodial wallet:
is a digital wallet arranged to store cryptocurrency; and/or
is provided by, in communication with and/or associated with the second network
20 entity.
16. A system, comprising:
a processor; and
memory including executable instructions that, as a result of execution by the processor,
25 causes the system to perform the method of any of the preceding claims.
17. A system according to claim 16 and further comprising:
an electronic recipient device associated with the recipient;
a computer-implemented network of nodes arranged for communication with each
30 other, and comprising nodes associated with the first, second and third network entities;
a non-custodial digital wallet associated with the user;
a security device such associated with the user and provided by the first network entity.

18. A non-transitory computer-readable storage medium having stored thereon executable instructions that, as a result of being executed by a processor of a computer system, cause the computer system to perform the computer-implemented method of any one of claims 1 to 16.