

## Claims

1. A computer implemented method for implementing at least one transaction associated with a distributed ledger, the at least one transaction being from sender for a recipient, whereby the sender and recipient are each associated with a respective payment entity among a plurality of payment entities that are communicatively coupled via a communication network, whereby each payment entity among the plurality of payment entities is a computing resource associated with a network identifier that is specific to said payment entity, the method comprising the steps of:
  - obtaining a public key P1 for the recipient;
  - verifying that the obtained public key P1 is associated with the network identifier of the recipient;
  - responsive to the verification being successful, calculating a further public key P2 pertaining to a given transaction based on the obtained public key, the given transaction associated with a digital asset;
  - computing a payment destination address for the recipient based on the further public (P2) key;
  - generating an output script for the given transaction based on the payment destination;
  - and
  - providing an unspent transaction output (UTXO) based on the output script to the distributed ledger.
2. The method as claimed in claim 1 wherein the output script includes a reference to the network identifier of the recipient.
3. The method as claimed in any one of claims 1 or 2 wherein the network identifier is a domain name of the recipient, said domain name being known to the sender, or being obtained from a network address of the recipient that is known to the sender.
4. The method as claimed in any preceding claim wherein the obtained public key P1 is part of a cryptographic key pair that includes a private key V1, such that one or more records associated with network identifier are encrypted with the private key V1.
5. The method as claimed in any preceding claim wherein the obtained public key P1 is digitally signed by a trusted authority (CA) to associate the obtained public key P1 to the

network identifier of the recipient, and wherein the step of verifying the obtained public key P1 is performed based on another public key associated with the trusted authority.

6. The method as claimed in claim 1 wherein the network identifier is a network address associated with the recipient, and wherein the obtained public key P1 is based on key exchange information associated with the network address.

7. The method as claimed in claim 6 wherein the step of verifying the obtained public key P1 is performed based on a certificate issued by a trusted authority (CA) for the network address.

8. The method as claimed in any preceding claim comprising:  
accessing a directory relating to a plurality of network identifiers;  
identifying a record associated with the network identifier of the recipient; and  
verifying the authenticity of the network identifier based on a security indicator present in the record.

9. A computer implemented method for implementing at least one transaction associated with a distributed ledger, the at least one transaction being from sender for a recipient, whereby the sender and recipient are each associated with a respective payment entity among a plurality of payment entities that are communicatively coupled via a communication network, whereby each payment entity among the plurality of payment entities is a computing resource, the method comprising the steps of:

determining a network address for the recipient, said network address being associated with a public key P1 for the recipient;

verifying that the network address is generated for, and is specific to the recipient;

responsive to the verification being successful, calculating a further public key P2 pertaining to a given transaction based on the public key for the recipient, the given transaction associated with a digital asset;

computing a payment destination address for the recipient based on the further public P2 key;

generating an output script for the given transaction based on the payment destination;  
and

providing an unspent transaction output (UTXO) based on the output script to the distributed ledger.

10. The method as claimed in claim 9 wherein the output script includes a reference to a network identifier of the recipient.
11. The method as claimed in any one of claims 9 or 10 wherein the network address for the recipient is a cryptographically generated address (CGA) derived from a cryptographic key pair including the public key P1, and a corresponding private key V1 associated with the recipient.
12. The method as claimed in claim 9 or 10 wherein the step of verifying the network address is based on a digital signature provided by a trusted authority (CA) for establishing a secure communication channel with the recipient.
13. The method as claimed in any one of claims 9 to 11 wherein the step of verifying the network address is based on a digital signature of the private key V2 that is included in a hash function used to generate the CGA for the recipient.
14. The method as claimed in any preceding claim wherein the step of calculating a further public key P2 comprises:
  - applying a secure hash function to a data item associated with the given transaction M to obtain a result, the data item M relating to the digital asset to be provided to the recipient; and
  - associating the public key P1 for the recipient with the result.
15. The method as claimed in any preceding claim wherein the step of computing the payment destination address includes computing a pay to public key hash (P2PKH) value based on applying a double hash function of the further public key P2, or wherein the step of computing a payment destination is based on a custom script associated with a public template for the recipient for digital assets transactions.
16. The method as claimed in any preceding claim wherein the step of providing the UTXO to the distributed ledger includes providing an additional non-spendable output having a locking script including the network identifier or network address of the recipient for the given transaction.
17. The method as claimed in any preceding claim comprising:

calculating a session key K1, wherein the session key is based on the further public key P2 for the given transaction, a private key V2 associated with the further public key and the public key P1 associated with the recipient;

encrypting a data item M of the given transaction with the session key K1, the data item M relating to the digital asset;

wherein the output script is generated based on the encrypted data item M.

18. A computer implemented method for implementing at least one transaction associated with a distributed ledger, the at least one transaction being from sender for a recipient, whereby the sender and recipient are each associated with a respective payment entity among a plurality of payment entities that are communicatively coupled via a communication network, whereby each payment entity among the plurality of payment entities is a computing resource, the method comprising the steps of:

obtaining a public key P1 for the recipient;

calculating a first public key P21 pertaining to a first transaction TX1 based on the obtained public key, the first transaction TX1 associated with a digital asset;

computing a first payment destination address for the recipient based on the first public P21 key;

calculating a first session key K1, wherein the first session key is based on the first public key P21 for the first transaction, a first private key V21 associated with the first public key P21 and the public key P1 associated with the recipient;

encrypting a data item M associated with the first transaction TX1 with the first session key K1, the data item M relating to the digital asset;

generating a first output script for the first transaction TX2 based on the encrypted data item M and the first payment destination address;

providing an unspent transaction output (UTXO) based on the output script to the distributed ledger;

calculating a second public key P22 pertaining to a second transaction TX2 based on the obtained public key P1, the second transaction associated with the UTXO of the first transaction;

computing a second payment destination address for the recipient based on the second public P22 key;

calculating a second session key K2, wherein the second session key K2 is based on the second public key P22 for the second transaction TX2, a second private key V22 associated with the second public key P22 and the public key P1 associated with the recipient;

encrypting the data item M associated with the first transaction TX1 with the second session key K2;

generating a second output script based on the encrypted data item M and the second payment destination; and

providing the second output script to the distributed ledger, wherein the second output is a non-spendable output.

19. A computer implemented method for implementing at least one transaction associated with a distributed ledger, the at least one transaction being from sender for a recipient, whereby the sender and recipient are each associated with a respective payment entity among a plurality of payment entities that are communicatively coupled via a communication network, whereby each payment entity among the plurality of payment entities is a computing device associated with a network identifier that is specific to said payment entity, the method comprising the steps of:

providing a public key P1 associated with the recipient, the public key further associated with a certificate issued by a trusted authority;

querying or monitoring the distributed ledger for one or more unspent transaction outputs (UTXO) associated with the recipient;

responsive to detecting a UTXO associated with the recipient, whereby the detected UTXO pertains to a given transaction, calculating a private key V2 for the given transaction, the private key V2 associated with a public key P2 for the given transaction;

processing a digital asset or processing a transfer of the digital asset by executing one or more output scripts in the detected UTXO to complete the given transaction; and

storing the completed transaction in the distributed ledger.

20. The method as claimed in claim 19 wherein the step of querying or monitoring the distributed ledger includes querying or monitoring for one or more UTXOs associated with the network identifier and/or a payment destination address of the recipient.

21. The method as claimed in any one of claims 19 or 20, wherein the step of calculating the private key for the detected UTXO comprises:

obtaining a private key V1 associated with the recipient, the private key being part of a cryptographic key pair associated with the public key P1 of the recipient;

computing the private key V2 for the given transaction based on the private key V1 of the recipient and a hash of a data item M associated with the given transaction, the data item M relating to the digital asset.

22. The method as claimed in any one of claims 19 to 21 wherein the step of querying or monitoring the distributed ledger comprises monitoring the distributed ledger for one or more

non-spendable outputs associated with the recipient, the additional outputs related to the detected UTXO.

23. The method as claimed in any one of claims 19 to 22 wherein the one or more UTXOs are provided to the distributed ledger by the sender according to the method as claimed in any one of claims 1 to 17.

24. The method as claimed in any one of claims 19 to 23 comprising:

- calculating a session key K1, wherein the session key is based on the public key and private key P2, V2 associated with the given transaction, and the public key P1 associated with the recipient;

- wherein the step of executing one or more output scripts includes decrypting a data item M associated with the given transaction in the one or more output scripts using the session key K1, the data item M relating to the digital asset.

25. A computer implemented method for implementing at least one transaction associated with a distributed ledger, the at least one transaction being from sender for a recipient, whereby the sender and recipient are each associated with a respective payment entity among a plurality of payment entities that are communicatively coupled via a communication network, whereby each payment entity among the plurality of payment entities is a computing device, the method comprising the steps of:

- providing a public key P1 associated with the recipient, the public key further associated with a certificate issued by a trusted authority;

- querying or monitoring the distributed ledger for one or more unspent transaction outputs (UTXO) associated with the recipient;

- responsive to detecting at least one UTXO associated with the recipient, whereby a detected UTXO among the at least one UTXOs pertains to a given transaction, the method further comprises:

- calculating a private key V2 for the given transaction, the private key V2 associated with a public key P2 for the given transaction;

- calculating a session key K1, K2 wherein the session key is based on the public key and private key P2, V2 associated with the given transaction, and the public key P1 associated with the recipient;

- decrypting a data item M associated with the given transaction in the detected UTXO using the session key K1, K2, wherein the data item M relates to a digital asset;

- executing one or more output scripts in the detected UTXO based on the decrypted data item M to complete the given transaction; and

storing the completed transaction in the distributed ledger.

26. The method as claimed in claim 25 wherein the step of detecting at least one UTXO includes detecting two UTXOs associated with the recipient, each UTXO relating to a respective transaction, and each UTXO being associated with the encrypted data item M; wherein one of the UTXO's is non-spendable output, such that said non-spendable output is used for identifying the other UTXO associated with a spendable output for a transfer of the digital asset.

27. The method as claimed any one of claims 19 to 26 comprising:

creating a record for the recipient in a directory relating to a plurality of network identifiers; and

updating or including an entry in the record with a security indicator associated with the network identifier of the recipient, said security indicator being provided for verifying the authenticity of the network identifier.

28. A computer implemented method for implementing at least one transaction associated with a distributed ledger, the at least one transaction being from sender for a recipient, whereby the sender and recipient are each associated with a respective payment entity among a plurality of payment entities that are communicatively coupled via a communication network, whereby each payment entity among the plurality of payment entities is a computing resource, the method comprising the steps of:

obtaining a network address for the recipient, said network address being generated in combination with a public key P1 for the recipient and a digital signature;

determining that the network address can accept digital assets;

responsive to said determination being successful, establishing a secure communication channel between the sender and the recipient;

requesting a payment destination address or a public template from the recipient;

responsive to obtaining the payment destination, generating an output script for a transaction pertaining to a digital asset; and

sending the output script to the payment destination.

29. A computer implemented method for implementing at least one transaction associated with a distributed ledger, the at least one transaction being from sender for a recipient, whereby the sender and recipient are each associated with a respective payment entity among a plurality of payment entities that are communicatively coupled via a communication network,

whereby each payment entity among the plurality of payment entities is a computing resource, the method comprising the steps of:

- responsive to an enquiry from the sender, providing a network address of the recipient for accepting digital assets, the network address being generated in combination with a public key for the recipient and a digital signature;

- establishing a secure communication channel between the sender and the recipient;

- generating a payment destination addresses or a public for the recipient;

- sending the payment destination address to the sender;

- obtaining an output script for a transaction pertaining to a digital asset from the sender;

and

- processing a payment relating to the digital asset; and

- creating a completed transaction based on the processed payment for the distributed ledger.

30. The method as claimed in claim 28 or 29 wherein the network address is a cryptographically generated address, and wherein the secure communication channel is established by deriving a session key for encrypting all communications sent to and/or received from the recipient.

31. The method as claimed in any one of claims 28 to 30 wherein the payment destination address is hash of a one-time public key for the digital asset (P2PKH).

32. The method as claimed in any one of claims 28 to 30 wherein public template includes a custom script generated for the recipient for obtaining a payment destination address associated with the recipient.

33. A computer implemented method for implementing at least one transaction associated with a distributed ledger, the at least one transaction being from sender for a recipient, whereby the sender and recipient are each associated with a respective payment entity among a plurality of payment entities that are communicatively coupled via a communication network, whereby each payment entity among the plurality of payment entities is a computing resource associated with a network identifier that is specific to said payment entity, the method comprising the steps of:

- querying a directory based on the network identifier of the recipient to resolve a network address for the recipient, wherein the network address being associated with a public key for the recipient, wherein the directory is associated with the communication network;

verifying that the network identifier of the recipient corresponds to a network identifier associated with the resolved network address for the recipient;

responsive to the verification being successful, performing the method step of any one of claims 7 to 17 or claim 28 for a given transaction.

34. The method as claimed in claim 33 wherein the network address is a cryptographically generated address and wherein the network identifier is a domain name for the recipient.

35. The method as claimed in any one of claims 33 or 34 wherein the network identifier is provided in an extension field associated with the network address.

36. A computing device, comprising:  
a processor; and  
memory including executable instructions that, as a result of execution by the processor, causes the system to perform the computer-implemented method of one of claims 1 to 18, 28, 30, 31 to 33 to 35.

37. A computing device, comprising:  
a processor; and  
memory including executable instructions that, as a result of execution by the processor, causes the system to perform the computer-implemented method of one of claims 19 to 27 or 29 to 32.

38. A system, comprising:  
one or more sender entities, each sender entity being a computing device according to claim 36;  
one or more recipient entities, each recipient entity being a computing device according to claim 37; and  
a communication network for facilitating communication between at least one sender entity and at least one recipient entity.

39. 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 35.