

Claims

1. A computer implemented method for use with a secure money transfer system which is operative to transfer funds, in a first currency, from a first (sending) bank account, at a first location, to a second (recipient) bank account at a second location, in which:

a first processing means identifies a sum of funds in the first account from where an amount of money is to be transferred;

a protocol buffer generates a block code in respect of the sum of funds to be transferred;

a memory stores the block code which includes data: identifying the sum of funds, a unique account identifier of the first sending bank account;

a communication device establishes a secure communication channel with a recipient account, at a recipient bank, to where the sum of funds is to be transferred;

a local transmission protocol buffer transmits the block code to a remote recipient protocol buffer via the secure communication channel;

the remote recipient protocol buffer receives the block code and transmits the block code to a bilateral synchroniser which relays account data and a liquidity check derived from the sending bank account to the recipient bank account;

a synchroniser synchronises the sending and receiving bank accounts thereby establishing a direct high speed connection therebetween;

upon receipt of an authorisation signal from the synchroniser a second processing means is operative to identify and ringfence the sum of funds in the first account from where the sum of funds is to be transferred;

when the sum of funds identified in the block code corresponds with the ringfenced sum of funds, an authorised user (account holder) is offered a transaction option for a predefined time period;

upon receipt of an input from the authorised user (account holder), confirming acceptance of the transaction option, a reciprocal arrangement is established

between the recipient bank account and the sending bank accounts for establishing a two way irrevocable authentication event thereby enabling funds to be transferred.

2. A method according to claim 1 wherein the funds that are paid into the second recipient bank account are paid in a different currency to the first currency.

3. A method according to claim 1 or 2 includes the step of transmitting to and/or from a protocol buffer via an encryption engine.

4. A method according to claim 3 includes the step of encrypting a message using an encryption engine which operates in accordance with a public private key encryption system protocol and/or an encryption algorithm, such as an RSA cryptographic algorithm.

5. A method according to any preceding claim wherein the unique account identifier of the first sending bank account is derived from the group comprising: an account number and a bank sort code; a bank identifier code (BIC); an international bank account number (IBAN); a country code number and one from a decentralised identity (DID).

6. A method according to any preceding claim wherein the user (account holder) is offered a transaction option for a predefined time period.

7. A method according to claim 6 wherein if the user (account holder) does not accept the transaction option offered within the predefined time period, a recalculation of the offer is derived by obtaining an updated liquidity check from the sending bank account.

8. A method according to any preceding claim wherein the user (account holder) is offered a transaction option in a user selectable currency recognised by the second (recipient) bank at the second location.
9. A method according to any preceding claim wherein upon receipt of an input signal, which includes an authorisation command from the user (account holder), confirming acceptance of a transaction, the funds to be transferred from the first (sending) bank account are ringfenced.
10. A method according to claim 9 wherein a processor determines at least a settlement charge, based upon the ringfenced sum of funds and at least a transaction charge which is based upon the value of a liquidity lock applied by the sending and/or receiving bank.
11. A method according to either claim 9 or 10 wherein a processor determines at least a transaction charge based upon the value of the liquidity lock applied by the sending and/or receiving bank.
12. A method according to claim 11 wherein the processor determines the value of the liquidity lock based upon an interbank risk factor.
13. A method according to any preceding claim wherein at least one gateway is established for connecting a proprietary payment system to the secure communication channel and includes one from the group comprising: a TCP/IP routing protocol gateway; remote protocol buffer, web socket, a virtual private network (VPN) and a SWIFT payment network.

14. A method according to any preceding claim includes establishing a data lake of transactional events which is populated in real time in a jurisdiction overseen by at least one central bank.

15. A method according to any preceding claim includes a web-based portal which is configured to deliver a menu to a display viewable by a user and from which a user command is transmitted to a communication network.

16. A method according to any preceding claim includes the step of identifying at least one participating bank and a specified currency suitable for use in the transaction by employing a currency matching and routing engine

17. A method according to any preceding claim wherein a participant bank employs a point-to-point encryption and communication network between protocol buffer components.

18. A method according to claim 17 wherein the protocol buffer operates in accordance with an encryption offloading sequence which is operable to transfer internal communications data, operating over an encrypted private infrastructure, to a public or proprietary network.

19. A method according to any preceding claim includes the step of logging communications from/to a protocol buffer to/from a bilateral synchroniser using a database and/or a distributed ledger or blockchain.

20. A method according to claim 19 includes the step of performing an audit log of stored data relating to communications between protocol buffers from/to a protocol buffer to/from a bilateral synchroniser.

21. A method according to any preceding claim includes the step of performing edge encryption of data.

22. A method according to any preceding claim includes the step of employing a distributed ledger which is located at a number of independent sites and/or in different countries and/or in independent institutions.

23. A system for transacting a secure money transfer which is operative to transfer funds, in a first currency, from a first (sending) bank account, at a first location, to a second (recipient) bank account at a second location, in which:

a first processing means identifies a sum of funds in the first account from where an amount of money is to be transferred;

a protocol buffer generates a block code in respect of the sum of funds to be transferred;

a memory stores the block code which includes data: identifying the sum of funds, a unique account identifier of the first sending bank account;

a communication device establishes a secure communication channel with a recipient account, at a recipient bank, to where the sum of funds is to be transferred;

a local transmission protocol buffer transmits the block code to a remote recipient protocol buffer via the secure communication channel;

the remote recipient protocol buffer receives the block code and transmits the block code to a bilateral synchroniser which relays account data and a liquidity check derived from the sending bank account to the recipient bank account;

a synchroniser synchronises the sending and receiving bank accounts thereby establishing a direct high speed connection therebetween;

upon receipt of an authorisation signal from the synchroniser a second processing means is operative to identify and ringfence the sum of funds in the first account from where the sum of funds is to be transferred;

when the sum of funds identified in the block code corresponds with the ringfenced sum of funds, an authorised user (account holder) is offered a transaction option for a predefined time period;

upon receipt of an input from the authorised user (account holder), confirming acceptance of the transaction option, a reciprocal arrangement is established between the recipient bank account and the sending bank accounts for establishing a two way irrevocable authentication event thereby enabling funds to be transferred.

24. A system according to claim 23 wherein the funds that are paid into the second recipient bank account are paid in a different currency to the first currency.

25. A system according to claim 23 or 24 includes an encryption engine which is operative to encrypt a transmission to and/or from a protocol buffer.

26. A system according to claim 25 wherein the encryption engine is operative in accordance with a public private key encryption system protocol and/or an encryption algorithm, such as an RSA cryptographic algorithm.

27. A system according to any of claims 23 to 26 wherein the unique account identifier of the first sending bank account is derived from the group comprising: an account number and a bank sort code; a bank identifier code (BIC); an international bank account number (IBAN); a country code number and one that can be derived from the use of a decentralised identity (DID).

28. A system according to any of claims 23 to 27 wherein a processor is operative to offer the user (account holder) a transaction option for a predefined time period.

29. A system according to claim 28 wherein a timer commences a time period and if the user (account holder) does not accept the transaction option offered within

the predefined time period, a recalculation of the offer is derived by obtaining an updated liquidity check from the sending bank account.

30. A system according to any of claims 23 to 29 wherein the user (account holder) is offered a transaction option, on a display, in a user selectable currency recognised by the second (recipient) bank at the second location.

31. A system according to any of claims 23 to 30 wherein upon receipt of an input signal, which includes an authorisation command from the user (account holder), confirming acceptance of a transaction, the system ringfences the funds to be transferred from the first (sending) bank account.

32. A system according to any of claims 23 to 31 wherein a processor determines at least a settlement charge, based upon the ringfenced sum of funds and at least a transaction charge which is based upon the value of a liquidity lock applied by the sending and/or receiving bank.

33. A system according to either claim 31 or 32 wherein a processor determines at least a transaction charge based upon the value of the liquidity lock applied by the sending and/or receiving bank.

34. A system according to claim 33 wherein the processor determines the value of the liquidity lock based upon an interbank risk factor.

35. A system according to any of claims 23 to 34 wherein at least one gateway is established for connecting a proprietary payment system to the secure communication channel and includes one from the group comprising: a TCP/IP routing protocol gateway; remote protocol buffer, web socket, a virtual private network (VPN) and a SWIFT payment network.

36. A system according to any of claims 23 to 35 includes a data lake of transactional events which is populated in real time in a jurisdiction overseen by at least one central bank.

37. A system according to any of claims 23 to 36 includes a web-based portal which is configured to deliver a menu to a display viewable by a user and from which a user command is transmitted to a communication network.

38. A system according to any of claims 23 to 37 includes a means that is operative to identify at least one participating bank and a specified currency suitable for use in the transaction by employing wherein a currency matching and routing engine identifies at least one participating bank and a specified currency.

39. A system according to any of claims 23 to 38 wherein a participant bank employs a point-to-point encryption and communication network between protocol buffer components.

40. A system according to claim 39 wherein the protocol buffer operates in accordance with an encryption offloading sequence which is operable to transfer internal communications data, operating over an encrypted private infrastructure, to a public or proprietary network.

41. A system according to any of claims 23 to 40 includes a means which logs communications from/to a protocol buffer to/from a bilateral synchroniser and includes a database and/or a distributed ledger or blockchain.

42. A system according to claim 41 includes a means that performs an audit log of stored data relating to communications between protocol buffers from/to a protocol buffer to/from a bilateral synchroniser.

43. A system according to any of claims 23 to 26 includes a means for edge encryption of data.

44. A system according to any of claims 23 to 43 includes a distributed ledger which is located at a number of independent sites and/or in different countries and/or in independent institutions.

45. A mobile telephone, tablet or laptop, includes a display and is operative in accordance with software and which is configured to communicate with the system according to any of claims 23 to 44.

46. A mobile telephone, tablet or laptop according to claim 45 has a biometric device that is operable by an authorised user to provide an input from the authorised user (account holder), confirming acceptance of a transaction.