

CLAIMS:

1. A computer-based system operative to use Simplified Payment Verification to facilitate a blockchain transfer of an asset between a transferor and a transferee, and comprising:
 - 5 at least one verification resource comprising at least one public key and arranged to receive and/or request, by the transferee and from the transferor:
 - complete transaction data relating to at least one blockchain transaction; and
 - a Merkle path for the at least one blockchain transaction;
 - a private key associated with the at least one public key; and
 - 10 a coordination component operative to communicate with the at least one verification resource.
2. A system in accordance with claim 1, wherein the private key is provided:
 - in the at least one verification resource; or
 - 15 in the coordination component.
3. A system in accordance with claim 1 or 2, wherein the verification resource is operative to:
 - verify whether a specified transaction is stored on a blockchain; and/or
 - 20 facilitate or enable a transfer from one address to another using a blockchain transaction.
4. A system in accordance with any preceding claim wherein the system comprises a plurality of verification resources and the coordination component is operative to
 - 25 select one verification resource from the plurality and cause it to:
 - verify whether a specified transaction is stored on a blockchain; and/or
 - facilitate or enable a transfer from one address to another using a blockchain transaction.
- 30 5. A system in accordance with any preceding claim wherein the coordination component is operative to send and receive transaction related data to and from a blockchain network.

6. A system in accordance with any preceding claim wherein the coordination component is operative to:
 - send and receive at least one public key and/or transaction ID (TXID) to and from the
 - at least one verification resource.
7. A system in accordance with any preceding claim wherein the private key is a seed.
8. A system in accordance with any preceding claim wherein the system comprises a plurality of verification resources, each comprising at least one public key associated with a respective private key.
9. A system in accordance with any preceding claim wherein the at least one verification resource is operative to:
 - i) use the Merkle path to verify a Merkle proof for the at least one transaction; or
 - ii) store, receive and/or request at least one block header of a blockchain transaction.
10. A system in accordance with any preceding claim wherein the complete transaction data or Merkle path are received and/or requested from a providing resource which is the transferor of the asset and is operative to store and/or send:
 - i) complete transaction data relating to the at least one blockchain transaction; and
 - ii) the Merkle path of the at least one blockchain transaction.
11. A system in accordance with any preceding claim wherein the providing resource and/or the verification resource is or comprises:
 - a digital wallet, a cryptocurrency wallet, a Simplified Payment Verification Wallet and/or a smart card.
12. A system in accordance with any preceding claim and operative to receive transfer data from a providing resource which is the transferor of the asset, the transfer data comprising:
 - data relating to at least one unspent transaction output (UTXO) stored on a blockchain;

a transaction ID (TXID) for a transaction containing the at least one unspent
blockchain transaction output (UTXO);
a signature for spending the at least one unspent blockchain transaction output
(UTXO);
5 a Merkle path for a transaction containing the at least one unspent blockchain
transaction output (UTXO); and/or
a public key address.

13. A system in accordance with any preceding claim wherein the system is operative to:

- 10 i) send a transfer value and/or an output address to a providing resource; and/or
ii) receive a transfer value and/or an output address from a providing resource which is
the transferor of the asset; and/or
iii) submit a transaction to a blockchain network upon successful verification of the
Merkle proof for the at least one blockchain transaction.

15

14. A system in accordance with any preceding claim wherein the system is operative to
send, to a providing resource which is the transferor of the asset, a request for transfer
data comprising at least one of:

- 20 data relating to at least one unspent transaction output (UTXO) stored on a
blockchain;
a transaction ID (TXID) for a transaction containing the at least one unspent
blockchain transaction output (UTXO);
a signature for spending at the at least one unspent blockchain transaction output
(UTXO);
25 a Merkle path for a transaction containing the at least one unspent blockchain
transaction output (UTXO); and/or
a public key address.

15. A system in accordance with claim 14 wherein the transfer data is requested by the
30 system, and/or received from the providing resource, using a blockchain transaction
template.