

CLAIMS:

1. A computer-implemented method of facilitating or enabling a transfer on a blockchain of an asset from a resource to a further resource, and comprising the step of providing, from the resource to the further resource:

complete transaction data relating to at least one blockchain transaction; and

a Merkle path for each input transaction that comprises at least one unspent blockchain transaction output that is spent as an input to the at least one blockchain transaction.

2. A method according to claim 1 wherein the resource and/or further resource comprises:

a digital wallet, a cryptocurrency wallet, or a lightweight or Simplified Payment Wallet; and/or

a computer-based device comprising a wallet; and/or

a smart card comprising a wallet.

3. A method according to claim 1 or 2 and further comprising the step of storing, receiving and/or generating, at or on the resource: at least one private key; and/or at least one public key.

4. A method according to any preceding claim and further comprising the step of receiving, at the resource, at least one block header.

5. A method according to any preceding claim, and further comprising the step of providing, by the resource to the further resource, transfer data comprising at least one of:

data relating to said each input transaction that comprises the at least one unspent blockchain transaction output (UTXO);

a transaction ID (TXID) for said each input transaction containing the at least one unspent blockchain transaction output (UTXO);

a signature for spending the at least one unspent blockchain transaction output (UTXO);

a public key address.

6. A method according to claim 5 wherein the transfer data is provided in response to a signal and/or request received from the further computer-implemented resource.
7. A method according to claims 5 or 6, wherein the transfer data is requested by the further resource, and/or provided by the resource, using a blockchain transaction template.
8. A method according to any preceding claim and further comprising the steps of:
 - sending a transfer value from the resource to the further resource; and/or
 - sending an output address from the resource to the further resource.
9. A method according to claim 8 and further comprising the step of updating the blockchain transaction template with:
 - at least one transaction ID (TXID) for an input transaction containing at least one unspent blockchain transaction output (UTXO); and/or
 - a signature for spending the at least one unspent transaction output (UTXO); and/or
 - a public key address.
10. A method according to claim 8 or 9 and further comprising the step of transmitting, from the resource to the further resource:
 - the updated blockchain transaction template;
 - at least one block header; and/or
 - the Merkle path for said each input transaction that comprises at least one unspent blockchain transaction output that is spent as an input to the at least one blockchain transaction.
11. A method according to any preceding claim and further comprising the step of storing, at or on the further resource:
 - the complete transaction data for the at least one blockchain transaction;
 - a transaction ID (TXID) for the at least one blockchain transaction; and/or

the Merkle path for said each input transaction that comprises at least one unspent blockchain transaction output that is spent as an input to the at least one blockchain transaction.

12. A method according to any preceding claim wherein the complete transaction data and the Merkle path for each input transaction that comprises at least one unspent blockchain transaction output that is spent as an input to the at least one blockchain transaction are sent from the resource to the further resource via an off-chain communication.
13. A method according to any preceding claim and further comprising the step of receiving, at the resource, a transfer value and/or an output address from the further resource.
14. A method according to any preceding claim and further comprising
using, by the further resource, the Merkle path for said each input transaction to perform a Simplified Payment Verification check on each said input transaction.
15. A method according to claim 14, comprising one or more of:
 - i) wherein the Simplified Payment Verification check is performed locally by the further resource without going through a blockchain network;
 - ii) wherein the method further comprises the step of broadcasting the at least one blockchain transaction to the blockchain network by the further resource;
 - iii) wherein the method further comprises performing step ii) only if the Simplified Payment Verification check performed on each said input transaction is affirmative.
16. A computer-implemented system comprising:
a processor; and
memory including executable instructions that, as a result of execution by the processor, causes the system to perform any embodiment of the computer-based method claimed in any of claims 1 to 15.

17. 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 at least perform an embodiment of the method as claimed in claims 1 to 15.