

CLAIMS:

1. A blockchain-implemented Simplified Payment Verification (SPV) method of using an SPV wallet to perform ~~comprising the steps~~:

5 receiving, from a computer-based resource via an off-chain communication, a Merkle path and complete transaction data for a first blockchain transaction comprising an unspent output;
 using the Merkle path and complete transaction data to verify ~~verifying a Merkle~~
 ~~proof for a~~ the first transaction comprising an unspent output (UTXO₁); and

10 sending a second transaction to a blockchain upon successful verification of the Merkle proof, wherein the second transaction comprises an input which spends the unspent output (UTXO₁) of the first transaction.

2. A method according to claim 1 and comprising the step of:

15 wherein the second transaction comprises at least one further input which spends at least one further unspent output (UTXO₂) of the first transaction or an unspent output (UTXO₃) of a third transaction.

3. A method according to claim 2 and comprising the step of:

20 verifying a Merkle proof for the third transaction.

4. A method according to ~~any preceding claim 2 or 3~~, and further comprising the step of:
 receiving, via an off-chain communication, a Merkle path and/or complete
 transaction data for the ~~at least one transaction and/or the third transaction~~.

25 5. A method according to any preceding claim, and further comprising the step of storing:
 at least one public key;
 at least one private key; and/or
 at least one block header.

30 6. A method according to any preceding claim, and further comprising the step of:

requesting, via an off-chain communication, the Merkle path and/or complete transaction data for the first transaction or third transaction from a computer-based resource.

5 7. A method according to claim 6 wherein the request is made using a transaction template.

8. A method according to claim 6 or 7 and further comprising the step of receiving, via an off-chain communication and from the computer-based resource:

10 the Merkle path and/or complete transaction data for the ~~first transaction or third~~ transaction;

a signature for spending at least one unspent blockchain transaction output (UTXO) of the first transaction and/or third transaction.

15 9. A method according to any preceding claim wherein the second transaction further comprises a change address for spending a portion of cryptocurrency to a destination.

10. A computer-implemented system comprising:

a processor; and

20 memory including executable instructions that, as a result of execution by the processor, causes the system to perform any embodiment of the computer-implemented method as claimed in any of claims 1 to 9.

25 11. A computer-implemented system according to claim 10 wherein the system comprises at least one Simplified Payment Verification wallet.

30 12. 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 any of claims 1 to 9.