

CLAIMS:

1. A blockchain implemented Simplified Payment Verification system operative to facilitate a transfer, over a blockchain network, of an asset on a blockchain between a transferor and a transferee, and comprising:
 - a first verification resource comprising:
 - complete transaction data relating to at least one blockchain transaction; and
 - the complete Merkle path of the at least one blockchain transaction.
 - and a second verification resource operative to:
 - receive and/or request, from the first verification resource, the complete transaction data relating to the at least one blockchain transaction; and the Merkle path for the at least one blockchain transaction;

and wherein the second verification resource is operative to:

 - receive and/or request, from the first verification resource, the complete transaction data and the Merkle path without accessing or communicating with the blockchain or the blockchain network.
2. A system according to claim 1 wherein the second verification resource is further operative to use the Merkle path to verify a Merkle proof for the at least one transaction.
3. A system according to claim 2 wherein the second verification resource is further operative to send a transfer transaction to the blockchain upon successful verification of the Merkle proof.
4. A system according to any preceding claim wherein the first and/or second verification resources are or comprise a smart card, digital wallet or a lightweight and/or SPV wallet.
5. A system according to any preceding claim wherein second verification resource is operative to receive and/or request, from the first verification resource, the complete transaction data and the Merkle path using an off-chain communication.
6. A system according to any preceding claim and operative to:
 - use the Merkle path to verify a Merkle proof for the at least one transaction and, upon successful verification, send a transaction to the blockchain.

7. A system according to any preceding claim wherein the system further comprises a plurality of second verification resources, and a coordination component operative to communicate with the plurality of verification resources.
8. A system according to any preceding claim wherein the first verification resource is the transferor of the asset and the second verification resource is the transferee of the asset.
9. A system according to any preceding claim wherein the second verification resource is also operative to receive and/or request from the first verification resource, or the first verification resource is also operative to send to the second verification resource at least one of:
 - a signature for spending an output of the at least one blockchain transaction;
 - a transfer value; and/or
 - a public key address.
10. A blockchain implemented method of Simplified Payment Verification to facilitate a transfer over a blockchain network of an asset on a blockchain between a transferor and a transferee comprising:
 - receiving, at a second verification resource and without accessing or communicating with the blockchain or the blockchain network:
 - complete transaction data relating to at least one blockchain transaction; and
 - the complete Merkle path of the at least one blockchain transaction;
 - wherein the transaction data and Merkle path are received from a first verification resource which stores the transaction data and Merkle path;
 - and preferably wherein the method further comprises the step of using the Merkle path to verify a Merkle proof for the at least one transaction.
11. The method of claim 10 and further comprising the step of sending a transfer transaction to the blockchain upon successful verification of the Merkle proof.
12. The method of claim 10 or 11 wherein the following steps are performed off-chain:
 - i) verification of the Merkle proof; and/or

- ii) receiving or requesting the complete transaction data and Merkle path from the first verification resource.
13. The method of claims 10 to 12, wherein the first verification resource is the transferor of the asset and the second verification resource is the transferee of the asset.
14. The method of claims 10 to 13 wherein:
- i) the second verification resource is operative to send a transaction to the blockchain upon successful verification of the Merkle proof; and/or
 - ii) the first and/or second verification resources are or comprise a smart card, digital wallet or a lightweight and/or SPV wallet.
15. 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 or system as claimed in any preceding claim.