CLAIMS

1. A computer-implemented method of authorising a payment by a target party to a verifying party, the method comprising, by the verifying party:

performing a payment verification to verify a source of funds of the target party, and outputting a result of true on condition that the target passes the payment verification;

performing an identity verification to verify an identity of the target party, the identity verification comprising:

- accessing response data stored in a data store in association with the identity of the target party, the data store being implemented in third party computer equipment of a trusted third party or on a peer-to-peer publication medium, wherein the response data comprises either a) a stored instance of a response to a challenge, or b) an attestation comprising a transformation of the response;

- sending a request comprising the challenge to the target party, and in response receiving back a further instance of the response; and

- performing a comparison and outputting a result of true on condition of a match, the comparison comprising either a) comparing the stored instance of the response with the further instance of the response, or b) comparing the attestation with the same transformation applied to the further instance of the response;

wherein the payment is authorised on condition that the outputs of both the payment verification and identity verifications is true.

2. The method of claim 1, wherein the response is a result of the challenge having been input, by a party other than the verifying party in a set-up phase preceding said method, into a PUF module comprising a physically unclonable function, PUF, which generated the stored response in dependence on the predetermined challenge using the PUF.

3. The method of claim 2, wherein the PUF module comprises a PUF and a deterministic transform function, and is configured to generate the response by:

- inputting a base input into the PUF to generate a corresponding base output; and

- inputting the challenge and into the transform function in conjunction with the generated base output in order to generate the response, the transform function being a function of the challenge and the generated base output.

4. The method of claim 2 or 3, wherein the party that performed the set-up was the target party.

5. The method of any preceding claim, wherein said request and receiving back are performed over a secure channel, secured based on a shared secret shared between the verifying party and the target party.

6. The method of any preceding claim, wherein the data store is implemented in the third party computer equipment.

~~7. The method of claim 6, wherein the third party computer equipment comprises server equipment comprising one or more server units at one or more geographic sites.~~

~~8~~7. The method of claim 6 ~~or 7~~ wherein the party that performed the set-up was the trusted third party.

~~9. The method of any of claims 6 to 8, wherein the response data is accessed from the data store of the third party computer equipment over a secure channel, secured based on a shared secret shared between the verifying party and trusted third party.~~

~~10~~8. The method of ~~any of claims 6 to 9~~claim 6 or 7, wherein the method comprises receiving the challenge and the response data from the trusted third party, said request sent by the verifying party comprising the challenge as received from the trusted third party.

~~11. The method of claim 10, wherein the challenge is received from the data store of the third party computer equipment over a secure channel, secured based on a shared secret shared between the verifying party and trusted third party.~~

~~12~~9. The method of any of claims 1 to 5, wherein the data store is implemented in the peer-to-peer publication medium.

~~13~~10. The method of claim ~~12~~9, wherein the peer-to-peer publication medium is a blockchain.

~~14~~11. The method of claim ~~13~~10, wherein the method comprises accessing the challenges and the response data from the blockchain, either directly from a node of a blockchain network or indirectly via one or more intermediate service providers, wherein said request sent by the verifying party comprises the challenge as received accessed from the blockchain.

~~15~~12. The method of claim ~~13~~10 or ~~14~~11, wherein the response data is stored in an output of a storage transaction recorded on the blockchain, and the identify verification further comprises checking that the response data has not been revoked by a further transaction having been recorded on the blockchain with an input pointing to an output of the storage transaction; wherein the output result of the identity verification is further conditional on the response data not having been revoked according to said checking.

~~16~~13. The method of claim ~~15~~12, wherein the response data is stored in a spendable output of the storage transaction and said checking comprises checking that the input of a further transaction does not revoke the response data by pointing to the same spendable output.

~~17~~14. The method of claim ~~15~~12, wherein the response data is stored in an unspendable output of the storage transaction and said checking comprises checking that the input of a further transaction does not revoke the response data by pointing to a spendable output in the same storage transaction.

~~18~~15. The method of any preceding claim, wherein the source of funds comprises one or more funding transactions recorded on a blockchain, the payment to be authorized comprising a spending transaction pointing to the funding transaction.

~~19~~16. The method of claim ~~18~~15, comprising, on condition that the results of both the payment verification and identity verification are true, providing a token to be included in a payload of the spending transaction evidencing the result of the identity verification.

~~20~~17. The method of claim ~~18~~15 or ~~19~~16, wherein the payment verification comprises a Simplified Payment Verification, SPV, process.

~~21~~18. The method of any preceding claim, wherein the method is performed from a point-of-sale terminal.

~~22~~19. Computer equipment comprising:

memory comprising one or more memory units; and

processing apparatus comprising one or more processing units, wherein the memory stores code arranged to run on the processing apparatus, the code being configured so as when on the processing apparatus to perform the method of any preceding claim.

~~23~~20. A computer program embodied on a non-transitory computer-readable medium and configured so as, when run on one or more processors, to perform the method of any of claims 1 to ~~21~~18.