

CLAIMS

1. A computer-implemented method for enabling one or more verifying parties to verify an identity of a target comprising a target party or device of the target party; the method comprising, in a set-up phase:

inputting of each of a set of one or more challenges into a PUF module comprising a physically unclonable function, PUF, to generate a respective one of a set of responses from each of the set of challenges; and

causing to be stored, on a blockchain, a respective piece of response data for each of the set of one or more responses generated by the PUF module, wherein the respective piece of response data for each response comprises the respective response or data derived therefrom, and wherein the pieces of response data are stored in one or more storage transactions recorded on the blockchain;

thereby making at least one of the pieces of response data available to the one or more verifying parties for verifying the identity of the target in a subsequent verification phase;

wherein the blockchain employs an output-based model whereby each of a plurality of transactions comprises at least one input and at least one output, each input pointing to an output of another transaction; and

wherein the method further comprises managing one or more of the pieces of response data by causing to be recorded, on the blockchain, a further transaction which comprises an input pointing to an output of one of the one or more storage transactions storing at least one of the pieces of the response data.

2. The method of claim 1, wherein the pieces of response data are stored in the one or more storage transactions together with one or more pieces of identification information identifying the target party.

3. The method of claim 1 or 2, wherein the method is performed by a trusted third party.

4. The method of claim 1 or 2, wherein the method is performed by the target party.
5. The method of claim 4, wherein said causing of the storage on the blockchain comprises: sending the at least one of the one or more storage transactions directly from the target party to a node of a blockchain network for recordal on the blockchain.
6. The method of any of claims 1 to 4, wherein said causing of the storage on the blockchain comprises: sending at least one of the one or more storage transactions to another party to forward on to a node of a blockchain network for recordal on the blockchain, or sending the set of responses or pieces of response data to another party to formulate at least one of the one or more storage transactions and forward on to a node of the blockchain network for recordal on the blockchain.
7. The method of any preceding claim, wherein the one or more verifying parties are a plurality of verifying parties.
8. The method of any preceding claim, wherein each piece of response data comprises an actual value of the respective response, thereby enabling a verifying party to verify the identity of the target by sending the respective challenge to the target party, receiving back a further instance of the respective response, and comparing with the value stored in the storage transaction on the blockchain.
9. The method of any of claims 1 to 7, wherein each piece of response data comprises an attestation of the respective response but does not disclose the respective response, wherein the attestation comprises a transformation of the respective response which enables a verifying party to verify the identity of the target by sending the respective challenge to the target party, receiving back a further instance of the respective response, applying the same transformation to the further instance of the response, and comparing with the attestation stored in the storage transaction on the blockchain.
10. The method of claim 9, wherein the transformation comprises a hash or double hash.

11. The method of any of claims 1 to 7, wherein each piece of response data comprises a public key of a respective public-private key pair derived from the respective response, which enables a verifying party to verify the identify of a message signed by the respective private key of the public-private key pair.

~~12. The method of any preceding claim, wherein the one or more pieces of response data are stored in the one or more storage transactions in encrypted form.~~

~~13. The method of any preceding claim, wherein the set of one or more challenges comprises a plurality of challenges, the set of responses comprising a respective plurality of responses.~~

~~14. The method of claim 13 as dependent on claim 12, wherein each of a plurality of subsets of the response data is encrypted with a different respective encryption key, each subset comprising a different respective one or more of the pieces of response data.~~

~~15. The method of claim 13 or 14, wherein the one or more verifying parties are a plurality of verifying parties, wherein only a respective subset of one or more of the pieces of response data is made available to each of the verifying parties.~~

~~16. The method of claim 15, wherein the subsets of verifying parties are exclusive of one another.~~

~~17. The method of claim 15 or 16, as dependent on claim 14, wherein the respective subsets are made available to the different verifying parties by distributing different decryption keys to different verifying parties.~~

~~18. The method of any of claims 13 to 17, wherein different ones of the pieces of response data are stored in different outputs of the same storage transaction.~~

~~19. The method of any of claims 13 to 17, wherein the one or more storage transactions comprise a plurality of storage transactions, and different ones of the pieces of response data are stored in different storage transactions.~~

~~20. The method of any preceding claim, wherein the blockchain employs an output-based model whereby each of a plurality of transactions comprises at least one input and at least one output, each input pointing to an output of another transaction.~~

2112. The method of any preceding claim ~~20~~, wherein each piece of response data is stored in ~~in~~ a spendable output of one of the one or more storage transactions.

2213. The method of claim ~~2120~~, wherein each piece of response data is embedded in a spendable output of one of the storage transactions by inclusion of an OP_RETURN or OP_DROP opcode in a script of the output.

~~2314.~~ The method of any preceding claim, wherein each piece of response data is stored in an unspendable output of one of the one or more storage transactions.

2415. The method of claim ~~2422~~, wherein the or each unspendable output is made unspendable by an OP_RETURN opcode, or OP_FALSE and OP_RETURN opcode, in a script of the output.

~~25. The method of any of claims 20 to 24, comprising managing one or more of the pieces of response data by causing to be recorded, on the blockchain, a further transaction which comprises an input pointing to an output of one of the one or more storage transactions storing at least one of the pieces of the response data.~~

2616. The method of any preceding claim ~~25~~, wherein said causing of the further transaction to be recorded on the blockchain comprises: sending the further transaction directly from the target party to a node of a blockchain network for recordal on the blockchain.

~~27~~17. The method of any preceding claim 25, wherein said causing of the further transaction to be recorded on the blockchain comprises: sending the further transaction to another party to forward on to a node of a blockchain network for recordal on the blockchain, or sending data for use in formulating the further transaction to another party to perform the formulation and forward on to a node of the blockchain network for recordal on the blockchain.

~~28~~18. The method of ~~claim 25 as dependent on claim 21~~20 or ~~22~~21, wherein the input of the further transaction points to a spendable output in which at least one of the pieces of response data is stored.

~~29~~19. The method of ~~claim 25, as dependent on claim 23~~22 or ~~24~~23, wherein the input of the further transaction points to a spendable output of a same transaction as that of an unspendable output in which at least one of the pieces of response data is stored.

~~30~~20. The method of claim ~~29~~27, wherein the at least one further transaction points to a spendable output of a same transaction as that of an unspendable output in which a plurality of the pieces of response data are stored, thus managing the plurality of pieces of response data at once.

~~31~~21. The method of any ~~of claims 20 to 30~~preceding claim, wherein the management comprises revoking the at least one piece of response data in the one or more pointed-to storage transactions, wherein the further transaction being recorded on the blockchain and pointing to the one or more pointed-to storage transactions causes the one or more verifying parties to deem the one or more pieces of response data stored therein as revoked.

~~32~~22. The method of any ~~of claims 20 to 31~~preceding claim, wherein the management comprises updating the at least one piece of response data in the one or more pointed-to storage transactions, the further transaction comprising a replacement version of the at least one piece of response data, wherein the further transaction being recorded on the blockchain and pointing to the one or more pointed-to storage transactions causes at least

one of the one or more verifying parties to replace the at least one piece of response data with the replacement version for use in the verification of the identity of the target.

~~33. The method of any preceding claim, wherein the one or more storage transactions further comprise an indication of the set of challenges, to enable each of the one or more verifying parties to determine a respective one of the set of challenges to use with a respective one of the responses in the verification, or to look up which of the set of responses to use with a given one of the set of challenges.~~

~~34. The method of claim 33, wherein the indication of the set of challenges comprises an actual value of each of the set of challenges each stored in association with its respective response.~~

~~35. The method of claim 33, wherein the indication of the set of challenges comprises a master challenge from which the set of challenges is derivable by applying a derivation function to the master challenge.~~

~~36. The method of any preceding claim, wherein the PUF module comprises the PUF, interface logic, and a deterministic transform function; wherein the interface logic causes the generation of the set of responses by:~~

~~—— receiving the set of challenges from said inputting;~~

~~—— inputting a base challenge into the PUF to generate a corresponding primary response; and~~

~~—— inputting each of the received set of challenges and into the transform function in conjunction with the generated base response in order to generate the respective response of said set of responses, the transform function being a function of the respective challenge from the received set and the generated base response.~~

~~37~~23. 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.

~~38~~24. 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 ~~36~~22.

~~39~~25. A computer-implemented method whereby a verifying party verifies an identity of a target comprising a target party or device of the target party; the method comprising, by the verifying party:

accessing response-related data having been generated by the target party having input a respective challenge to a PUF module comprising a physically unclonable function, PUF, to generate the response based on the PUF, wherein the response-related data comprises the response or data derived therefrom; and

verifying the identity of the target based on the accessed piece of response data;

wherein the response-related data is stored on a blockchain maintained by a blockchain network, and said accessing comprises accessing the response-related data from the blockchain, either directly from a node of a blockchain network or via one or more intermediate service providers.

~~40. The method of claim 39, wherein the response data comprises either: a) an actual value of the response, or b) an attestation comprising a transformation of the response; and the verifying comprises:~~

~~— sending to the target a request comprising one of the set of challenges to the target, and in response receiving back a further instance of the response; and~~

~~— performing a comparison and verifying the identity of the target on condition that the comparison results in a match, wherein the comparison comprises: in the case of a) the accessed value of the response matches the further instance, or in the case of b) the attestation matches the same transformation applied to the further instance.~~

41. — The method of claim 39 or 40, further comprises detecting on the blockchain a further transaction pointing to at least one of the storage transactions, and based thereon deeming the piece or pieces of response data stored in the at least one storage transaction to be either revoked or updated with a replacement version stored in the further transaction.

42. — 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 claim 39, 40 or 41.

43. — 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 claim 39, 40 or 41.

44. — A node of a blockchain network storing at least part of a blockchain, including one or more storage transactions storing, in association with one or more pieces of identification information identifying a target, respective response-related data for each of one or more responses generated by a PUF module comprises a physically unclonable function, PUF, each response having been generated based on the PUF in response to a respective challenge, wherein the respective response-related data for each response comprises the respective response or data derived therefrom.

45. — A blockchain transaction embodied on a non-transitory computer-readable medium, wherein the blockchain transaction includes, in association with one or more pieces of identification information identifying a target, respective response-related data for each of one or more responses generated by a PUF module comprises a physically unclonable function, PUF, each response having been generated based on the PUF in response to a respective challenge, wherein the respective response-related data for each response comprises the respective response or data derived therefrom.