

CLAIMS:

1. A computer-implemented method comprising the steps:
generating a plurality of multiparty computational challenges;
5 providing each mining node in a plurality of mining nodes on a Proof-of-Work
blockchain network with a respective challenge from the plurality of multiparty
computational challenges;
wherein:
the respective challenge comprises the calculation of an RSA modulus that is used
10 in a repeated squaring time-lock puzzle.
2. A method according to claim 1 wherein:
each challenge in the plurality of multiparty computational challenges requires the
use of an inherently sequential algorithm to find a solution to the challenge.
15
3. A method according to claims 1 or 2 and further comprising the step of:
generating a plurality of further multiparty computational challenges;
providing each mining node in the plurality of mining nodes with a respective further
challenge from the plurality of further multiparty computational challenges.
20
4. A method according to claim 3, wherein the steps of claim 3 are performed when a
solution has been found, by one of the mining nodes in the plurality of mining nodes, to
a multiparty computational challenge or a further multiparty computational challenge.
- 25 5. A method according to any preceding claim wherein:
generation of the plurality of multiparty computational challenges and/or the plurality of
further multiparty computational challenges is performed, at least in part, by a
subset of computer-based entities which is selected from a plurality of computer-
based entities.
30
6. A method according to claim 5 wherein at least one of the computer-based entities is a
mining node on the blockchain network.

7. A method according to claims 5 or 6 wherein the subset of computer-based entities is selected from the plurality of computer-based entities according to a random or pseudo-random selection process.
- 5 8. A method according to any preceding claim wherein:
the generation of at least one of the multiparty computational challenges and/or further multiparty computational challenges comprises the calculation of an output to an operation which uses a random or pseudo-random input.
- 10 9. A method according to any preceding claim wherein:
the generation of at least one of the multiparty computational challenges and/or further multiparty computational challenges comprises the generation of an RSA key pair.
10. A method according to any preceding claim and further comprising the step of using an
15 inherently sequential algorithm to find a solution to at least one of the multiparty computational challenges and/or further multiparty computational challenges.
11. A method according to claim 10 wherein the inherently sequential algorithm comprises at least one of the following operations:
20 a recursive operation;
a modular exponentiation;
a repeated squaring operation.
- 25 12. 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-implemented method as claimed in any of claims 1 to 11.
30
13. A computer implemented system according to claim 12 wherein the system comprises a plurality of nodes on a blockchain network, at least one of the nodes comprising the processor, memory and executable instructions of claim 12.

14. 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 11.