

CLAIMS

1. A method comprising the steps of:

generating or receiving, at a first space-time point, a plurality of random quantum states, each of the quantum states chosen from a set of non-orthogonal quantum states;

5 applying a pre-determined measurement, from a plurality of possible pre-determined measurements, to the quantum states in order to obtain a token comprising a sequence of classical measurement outcomes;

receiving, at a second space-time point in the causal future of the first space-time point, the token comprising a sequence of classical measurement outcomes; and

10 verifying whether the token corresponds to a statistically plausible result for the predetermined measurement applied to the plurality of quantum states, before allowing access to a resource.

2. The method of claim 1, wherein the quantum states are chosen independently randomly from among the pure states of a plurality of possible bases for the quantum state space.

15 3. The method of any preceding claim, wherein the quantum states represent quantum bits, qubits.

4. The method of claim 3, wherein each of the plurality of quantum states comprises a BB84 state for the corresponding two-dimensional qubit space.

20 5. The method of claim 3 or claim 4, wherein each of the plurality of qubits is encoded in a photon of electromagnetic energy.

6. The method of claim 5, wherein each qubit is encoded as a polarisation state of the corresponding photon.

7. The method of claim 5, wherein each qubit is represented by the polarisation state of a weak light pulse with low expected photon number.

25

8. The method of any preceding claim, wherein the pre-determined measurement comprises a projection of each of the plurality of quantum states onto one of the possible pure states of the corresponding quantum state space.
- 5 9. The method of any preceding claim, wherein the pre-determined measurement is such that the possible measurement outcomes give a valid token for the second space-time point.
- 10 10. The method of claim 9, wherein the probability that the result of the pre-determined measurement gives a valid token for a third space-time point separated from the second space-time point is small.
- 11 11. The method of claim 10, wherein the probability that the result of the pre-determined measurement gives a valid token for the third space-time point is negligible.
- 12 12. The method of any preceding claim, further comprising encrypting the token prior to receiving the token.
- 13 13. The method of any preceding claim, wherein the plurality of quantum states are entangled; 14. The method of any preceding claim, wherein the plurality of quantum states
15 comprises at least around 10^3 quantum states.
- 15 15. The method of any preceding claim, further comprising transmitting data identifying the states for which the measurement was successful.
- 16 16. The method of any preceding claim, further comprising receiving data identifying the states for which the measurement was successful.
- 20 17. The method of any preceding claim, further comprising receiving, at a fourth space-time point in the future of the first space-time point and in the past of the second space-time point, a second plurality of quantum states; applying a second pre-determined measurement to the second plurality of quantum states to obtain a second sequence of classical measurement outcomes; appending the second sequence of classical measurement outcomes to the token; and
25 presenting, at the second space-time point, the extended token in return for access to the resource.

18. The method of claim 17 including iterating, at each of a plurality of successive timelike separated space-time points in the future of the first space-time point and in the past of the second space-time point, the steps of receiving a further plurality of quantum states, applying a pre-determined measurement to the plurality of quantum states to obtain a further sequence of classical measurement outcomes, and appending the further sequence of classical measurement outcomes to the token, such that the token presented at the second space-time point comprises each of the plurality of sequences of classical measurement outcomes.

19. The method of any preceding claim, further comprising generating, at a fourth space-time point in the future of the first space-time point and in the past of the second space-time point, a second plurality of quantum states; wherein verifying whether the token corresponds to a statistically plausible result for a pre-determined measurement comprises verifying whether the token includes a statistically plausible result for a first predetermined measurement on the first plurality of quantum states and a statistically plausible result for a second pre-determined measurement on the second plurality of quantum states.

20. The method of claim 19 including iterating, at each of a plurality of successive timelike separated space-time points in the future of the first space-time point and in the past of the second space-time point, the step of generating a further plurality of quantum states; wherein receiving the token comprising a sequence of classical measurement outcomes comprises receiving an extended token comprising a plurality of sequences of classical measurement outcomes, and wherein verifying whether the token corresponds to a statistically plausible result for a pre-determined measurement comprises verifying whether the token includes a statistically plausible result for each of a plurality of respective pre-determined measurements on each generated plurality of quantum states.

21. The method of any preceding claim, comprising receiving, at the first space-time point, multiple pluralities of random quantum states, each of the quantum states chosen from a respective set of non-orthogonal quantum states; applying a respective predetermined measurement to the quantum states to obtain an extended token comprising a number of sequences of classical measurement outcomes; and presenting, at the second space-time point, a portion of the extended token in return for access to a resource.

22. The method of any preceding claim, comprising generating, at the first space-time point, multiple pluralities of random quantum states, each of the quantum states

chosen from a respective set of non-orthogonal quantum states; receiving, at a second space-time point in the causal future of the first space-time point, an extended token comprising a number of sequences of classical measurement outcomes; and verifying whether the token corresponds to a statistically plausible result for respective pre-determined measurements on each of the pluralities of quantum states.

5