

SUMMARY OF THE INVENTION

The invention is defined in the independent claims, to which reference is now directed.

Preferred features are set out in the dependent claims.

In its broadest aspect, the invention provides a scheme that uses quantum information to obtain
5 some of the important advantages of quantum money just outlined, in a way that is
technologically feasible today. In particular, the token itself in the present schemes is classical,
so that the invention does not rely on the presently problematic long-term storage or
transportation of quantum states. In spite of this, embodiments of the invention provide a token
that cannot be copied, and which is limited in transmission speed only by the light signalling
10 bound. According to the invention, the future privacy of the token recipient may be respected;
and certain embodiments within the scope of the invention may also guarantee past privacy.

According to one aspect of the invention, there is provided 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, and applying a pre-
15 determined measurement to the quantum states to obtain a token comprising a sequence of
classical measurement outcomes that is valid at a single space-time point. The method further
includes the step of 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
verifying whether the token corresponds to a statistically plausible result for the predetermined
20 measurement applied to the plurality of quantum states, before allowing access to a resource.

According to another aspect of the invention, there is provided a method comprising the steps of
generating, 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, and receiving, at a
second space-time point in the causal future of the first space-time point, a token comprising a
25 sequence of classical measurement outcomes. The method further includes the step of
verifying whether the token corresponds to a statistically plausible result for a pre-determined
measurement of the quantum states.

References herein to events or to the performance of method steps 'at' a space-time point are
intended to comprise occurrences within an agreed, small (four-dimensional) region around the
30 relevant point. For example, as the skilled person will appreciate the exchange of information
generally requires classical and/or quantum data to be sent through agreed channels between
two nearby secure sites controlled respectively by either of the parties to the exchange.

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 that is valid at a single space-time point;

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