DR. PETER SHOR, MIT

Quantum Money

Quantum money is a quantum cryptograph protocol with several players, one of whom we call the mint. We assume all participants have quantum computers. For a quantum money protocol, we need

1. The mint must be able to create a quantum money state (with an associated serial number)

2. A merchant holding the quantum money state and knowing the serial number must be able to verify that it is a valid quantum money state.

3. An aspiring counterfeiter having both the quantum money and the serial number cannot create two states which both pass the verification test.

Quantum money was first proposed in 2009. Since then, a number of quantum money schemes have been proposed, several of which have been broken. We will discuss the history of quantum money and sketch how some of the schemes work.