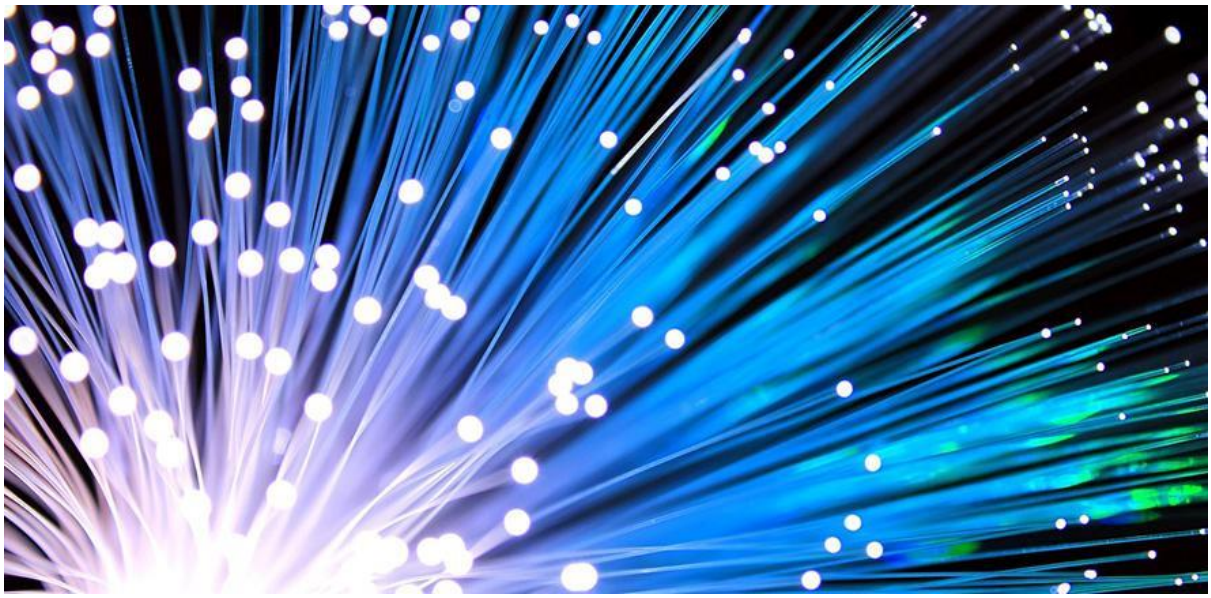
Ultra-secure form of virtual money proposed

8 May 2019

A new type of money that allows users to make decisions based on information arriving at different locations and times, and that could also protect against attacks from quantum computers, has been proposed by a researcher at the University of Cambridge.



Fiber Optic Cable Blue Credit: chaitawat

The theoretical framework, dubbed 'S-money', could ensure completely unforgeable and secure authentication, and allow faster and more flexible responses than any existing financial technology, harnessing the combined power of quantum theory and relativity. In fact, it could conceivably make it possible to conduct commerce across the Solar System and beyond, without long time lags, although commerce on a galactic scale is a fanciful notion at this point.

Instead of something that we hold in our hands or in our bank accounts, money could be thought of as something that you need to get to a certain point in space and time.

- Adrian Kent

Researchers aim to begin testing its practicality on a smaller, Earth-bound scale later this year. S-money requires very fast computations, but may be feasible with current computing technology. Details are published in the Proceedings of the Royal Society A.

"It's a slightly different way of thinking about money: instead of something that we hold in our hands or in our bank accounts, money could be thought of as something that you need to get to a certain point in space and time, in response to data that's coming from lots of other points in space and time," said Professor Adrian Kent, from Cambridge's Department of Applied Mathematics and Theoretical Physics, who authored the paper.

The framework developed by Professor Kent can be thought of as secure virtual tokens generated by communications between various points on a financial network, which respond flexibly to real-time data across the world and 'materialise' so that they can be used at the optimal place and time. It

allows users to respond to events faster than familiar types of money, both physical and digital, which follow definite paths through space.

The tokens can be securely traded without delays for cross-checking or verification across the network, while eliminating any risk of double-trading. One way of guaranteeing this uses the power of quantum theory, the physics of the subatomic world that Einstein famously dismissed as "spooky".

The user's privacy is maintained by protocols such as bit commitment, which is a mathematical version of a securely sealed envelope. Data are delivered from party A to party B in a locked state that cannot be changed once sent and can only be revealed when party A provides the key – with security guaranteed, even if either of the parties tries to cheat.

Other researchers have developed theoretical frameworks for 'quantum' money, which is based on the strange behaviour of particles at the subatomic scale. While using quantum money for real world transactions may be possible someday, according to Kent, at the moment it is technologically impossible to keep quantum money secure for any appreciable length of time.

"Quantum money, insofar as it's currently understood, would require long-term storage of quantum states, or quantum memory," said Kent. "This would require an awful lot of resources, and even if it becomes technologically feasible, it may be incredibly expensive."

While the S-money system requires large computational overhead, it may be feasible with current computer technology. Later this year, Kent and his colleagues hope to conduct some proof-of-concept testing working with the Quantum Communications Hub, of which the University of Cambridge is a partner institution. They hope to understand how fast S-money can be issued and spent on a network using off-the-shelf technologies.

"We're trying to understand the practicalities and understand the advantages and disadvantages," said Kent.

Patent applications for the research have been filed by Cambridge Enterprise, the University's commercialisation arm.

Reference:

Adrian Kent. 'S-money: virtual tokens for a relativistic economy.' Proceedings of the Royal Society A (2019). DOI: 10.1098/rspa.2019.0170