conferenceseries.com

Aleksey Fedorov, J Laser Opt Photonics 2017, 4:3(Suppl)
DOI: 10.4172/2469-410X-C1-014

2nd International Conference on

Quantum Physics and Quantum Technology

September 25-26, 2017 Berlin, Germany

Quantum key distribution networks and their applications for blockchain-based technologies

Aleksey Fedorov
Russian Quantum Center, Russia

The blockchain is a distributed ledger platform with high Byzantine fault tolerance, which enables achieving consensus in a large decentralized network of parties who do not trust each other. A paramount feature of blockchains is the accountability and transparency of transactions, which makes it attractive for a variety of applications ranging from smart contracts and finance to manufacturing and healthcare. Blockchain relies on two one-way computational technologies: hash functions and digital signatures. Most blockchain platforms rely on the elliptic curve public-key cryptography or the integer factorization problem to generate a digital signature. The security of these algorithms is based on the assumption of computational complexity of certain mathematical problems. A universal quantum computer would enable efficient solving of these problems, thereby making digital signatures, including those used in blockchains, insecure. A way to guarantee authentication in the quantum era is to use quantum key distribution, which guarantees information-theoretic security based on the laws of quantum physics. Quantum key distribution is able to generate a secret key between two parties connected by a quantum channel (for transmitting quantum states) and a public classical channel (for post processing). In this contribution, we describe a blockchain platform that is based on quantum key distribution and implement an experiment demonstrating its capability in a three-node urban quantum key distribution network. We believe this scheme to be robust against not only the presently known capabilities of the quantum computer, but also those that may potentially be discovered in the future to make post-quantum cryptography schemes vulnerable. The utility of quantum key distribution for blockchains may appear counterintuitive, as quantum key distribution networks rely on trust among nodes, whereas the earmark of many blockchains is the absence of such trust. Employing quantum key distribution for communication between two parties via a direct quantum channel permits these parties to authenticate each other. That is, nobody can pretend to be somebody else when introducing a transaction. Quantum key distribution, in combination with classical consensus algorithms, can be then used in lieu of classical digital signatures.

Biography

Aleksey Fedorov graduated from Bauman Moscow State Technical University (MS, 2016) and COMPLETED PhD from University of Paris-Saclay (2017). For excellent academic achievements, he was awarded by a number of prestigious scholarships such as Russian Federation Government Scholarship (2013-2014), Russian President Scholarship (2014-2015), Bauman University Scientific Committee Scholarship (2014), Bauman University Alumni Club Scholarship (2015), and many others. His research activities were recognized by the RQC fellowship for undergraduate students (2013-2015) and the Dynasty Foundation Fellowship for undergraduate students (2014-2015). Research interests are at the interface of quantum optics, atomic and molecular physics, condensed matter physics, and quantum information science.

akf@rqc.ru

Notes: