Maintaining quantum-secured blockchain with urban fiber quantum key distribution network

E.O. Kiktenko[1,2], N.O. Pozhar[1], M.N. Anufriev[1], A.S. Trushechkin[1,2], R.R. Yunusov[1], Y.V. Kurochkin[1],A.I. Lvovsky[1,3] and A.K. Fedorov[1,4]

[1]*Russian Quantum Center, Skolkovo, Moscow 143025, Russia*
[2]*Steklov Mathematical Institute of Russian Academy of Sciences, Moscow 119991, Russia*
[3]*Institute for Quantum Science and Technology, University of Calgary, Calgary AB T2N 1N4, Canada*
[4]*LPTMS, CNRS, Univ. Paris-Sud, Université Paris-Saclay, Orsay 91405, France*
e-mail: *e.kiktenko@rqc.ru*

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 [1].

The modern blockchain technology relies on one-way cryptographic primitives such as ECDSA or RSA which are vulnerable to attacks with a universal quantum computer. One of the ways to guarantee authentication in the quantum era is to use quantum key distribution (QKD), which guarantees information-theoretic security based on the laws of quantum physics [2]. In the current contribution (see [3] for more details), we describe a blockchain platform that is based on QKD and implement an experiment demonstrating its capability in a three-node urban QKD 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.

We consider a blockchain protocol within a twolayer network with n nodes. The first layer is a QKD network with pairwise communication channels that permit establishing information-theoretically secure private key for each pair of nodes. The second (classical) layer is used for transmitting messages with authentication tags based on Toeplitz hashing that are created using the private keys procured in the first layer.

The operation of the blockchain is based on two procedures: (i) creation of transactions and (ii) construction of blocks that aggregate new transactions. In the first procedure a new transaction, authored by one of the nodes, is sent via authenticated channels to all other $n-1$ nodes, thereby entering the pool of unconfirmed transactions. For the second procedure, we employ the broadcast protocol proposed in the classic paper by Shostak, Lamport and Pease [4]. This protocol allows achieving a Byzantine agreement in any network with pairwise authenticated communication provided that the number of dishonest parties is less than $n/3$ (which we assume to be the case).

We experimentally study the proposed blockchain protocol on the basis of a $n=4$ node, six-link network [Fig. 1(a)] with information-theoretically secure authentication. We use an urban fiber QKD network recently developed by our team [5] to procure authentication keys for two of the links connecting three nodes; the key generation in the remaining four links is classical. We test the operation of the blockchain and implement the construction of a simple transaction block in a settings, where node D tries to process three inconsistent transactions, i.e. realize a “double-spending” attack [Fig. 2(b)]. The protocol eliminates node D’s double-spending transaction after the broadcast procedure and permits the formation of a block containing legitimate transactions only [Fig. 2(c)].

In summary, we have developed a blockchain protocol with information-theoretically secure authentication based on a network in which each pair of nodes is connected by a QKD link. We have experimentally tested our protocol by means of a three-party urban fibre network QKD in Moscow. A crucial advantage of our blockchain protocol is its ability to maintain transparency of transactions and security against attacks with quantum algorithms. Our results therefore open up possibilities for realizing scalable quantum-safe blockchain platforms. If realized, such a blockchain platform can limit economic and social risks from imminent breakthroughs in quantum computation technology.

References

[1] P. Franco, *Understanding Bitcoin: Cryptography, Engineering and Economics* (John Wiley & Sons, 2014).

[2] E. Diamanti, H.-K. Lo, and Z. Yuan, npj Quant. Inf. **2**, 16025 (2016).

[3] E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.I. Lvovsky, and A.K. Fedorov, arXiv:1706.00611.

[4] M. Pease, R. Shostak, and L. Lamport, ACM T. Progr. Lang. Sys., **4**, 382 (1982).

[5] E.O. Kiktenko, N.O. Pozhar, A.V. Duplinskiy, et al. arXiv:1705.07154.

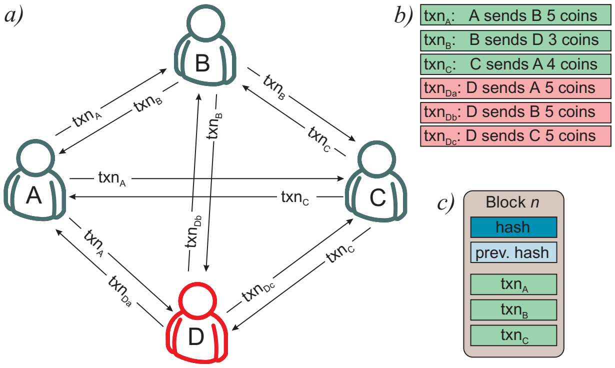

Figure 1: Creation of a block in a quantum-secure blockchain. a) Each node who wishes to implement a transaction sends identical copies of that transaction to all other nodes. Nodes A, B and C, whose transactions are denoted as txn_A, txn_B and txn_C, respectively, follow the protocol. Node D is cheating, attempting to send non-identical versions txn_Da, txn_Db and txn_Dc of the same transaction to different parties. b) Transaction contents. c) The nodes implement the broadcast protocol to reconcile the unconfirmed transactions and form the block. They discover that the transaction initiated by node D is illegitimate and exclude it.