Quantum Proof Blockchain Ledger

Patel Manish
Edumonk Foundation, E-41, Panchsheel Park, South Delhi, INDIA
manish@edumonk.org

Abstract

This study aims to resolve the vulnerabilities associated with the cryptocurrencies and blockchain ledgers due to the enormous computing power quantum computing would bring to the world. Most of the protocols used in the development of blockchains and cryptocurrencies involve using a public key system based on Elliptical Curve Cryptography based on finding numbers on an elliptical curve.

The most common signature schemes used are DSA, ECDSA and RSA which are quite vulnerable to quantum attack. It is a very alarming situation for thriving crypto economy to keep the wealth of people safe in different wallets they are using for storing their cryptocurrency.

Keywords: Quantum Proof Ledger, QUBITS, Shor's Algorithm, Proof of Stake System.

Introduction

Bitcoin is a decentralized online cash system and its developed versions have been widely used in the modern society as an alternative of traditional currency. However, its security basically relies on cryptography based on the computation hardness assumptions in terms of classical computers and recent advances on quantum computers constituting a grave menace to the safety. It is believed that quantum computers can hasten the mining process and may crack the SHA256 hash algorithm used by Bitcoin network.

Actually, it is reported that the classical signature scheme used by Bitcoin is at risk and could be completely broken by quantum attack within a couple of decades. Even though it may not mean Bitcoin faces immediate danger of being hacked by a quantum computer, no one will doubt there is a potential danger. Of course, the similar problem is true of banks all over the world. In order to solve this issue, we try to transplant it on a quantum network and to quantize the whole system by use of all quantum technologies which keep on evolving. Novelty of qBitcoin compared to Bitcoin or other quantum money schemes can be summarized as follows:

1. Quantum teleportation is used to transmit a coin. This prevents from double spending in a simple way without help of a blockchain.

2. Quantum digital signature is used to verify transaction. This requires other participants to be involved in verifying signatures, hence it is compatible with P2P.

3. Transaction can be completed much faster than Bitcoin. Each node is not a block but a point, hence transaction is immediately completed once if signature is verified.

First of all, we need to consider how to transmit a coin made of quantum information. The best way, at the present, will be to employ quantum teleportation[3-6], which is succeeded in transforming quantum information to remote places. Great benefit to use the quantum teleportation is that the quantum information cannot remain at the original place, in other words, it is impossible for a transmitter to keep the original quantum data once the quantum information is sent. This point is quite useful for coin transaction since any coin data should not be 2 duplicatable and this gives a strong advantage to qBitcoin.

Quantum money we employ is not to be forged, therefore so-called the double spending problem never occurs on qBitcoin. On the other hand, this issue was crucial in Bitcoin and the blockchain system was invented to solve it. However, this causes another problem: making a block is time-consuming and one needs to wait more than 10 minutes to complete a transaction. qBitcoin is made of a network connecting points, rather than blocks. Therefore, the quantized system will succeed in transmitting money much faster than Bitcoin.

Secondly, we should mention security. As most commonly discussed, it is vital to maintain the system so that it is tolerant to hacking by a third party. In the conventional banking systems including Bitcoin, their security systems rely on cryptography whose security is guaranteed temporarily by the computational hardness assumption as represented by integer factorization algorithms and elliptic curve cryptography. However, it is widely known that a quantum computer manages to break such conventional code in a short time. So, it is wise to find an alternative method. In qBitcoin, we employ quantum cryptography which is secure since it is protected by the laws of physics, hence it is secure forever in principle. Moreover, owner's privacy can be perfectly protected in such a way that his/her private information is not leaked out due to blind quantum computation.[7-9] This makes the system robuster by far than the conventional Bitcoin.

Thirdly, it is also important to inherit the crucial property of Bitcoin to qBitcoin; the peer to peer (P2P) system, since this makes different from the traditional banking system, namely Bitcoin succeeded in establishing an online cash system without a help of an authorized third party. We consider a novel signature verification system based on quantum digital signature.

Coin: A coin is defined by a pair of classical and quantum states ci = (ri , |ψii) where i labels a serial number and ri is a transaction record made of clas- 3 sical bits and transaction is done by passing ci to another person. These classical bits ri and quantum bits (qubits) |ψii given to coins should be one-to-one correspondence so that no one can duplicate. Namely, they obey ri 6= rj ⇔ |ψii 6= |ψj I for all serial numbers i, j. What is different form the usual currency or Bitcoin is that such quantum information about the coin is hidden to anybody. The mint derivers quantum coins to those who want to trade. Owners of coins can possess the quantum state but cannot obtain full information to forge.

Moreover, the no-cloning theorem helps the system prevent owners from making copies of coins. Even if full quantum information is not opened to the public, one can transport the information to somebody else using quantum teleportation. Those serial numbers should be authenticated without contact with a central authority. Such a quantum money scheme has the desired properties:

1. Anyone can verify money given by the mint but cannot forge it.

2. Anyone can authenticate the serial numbers.

Transactions

Remittance: In qBitcoin, quantum information of a coin and a bank statement is transmitted by use of quantum teleportation[3], which is a protocol to send quantum information to remote locations via classical information network. Experimental techniques are already established.[5,6] The procedure to transmit a coin is as follows: Let |ψi be a coin which a remitter wants to send to a receiver. The remitter and the receiver share a EPR pair and the remitter performs a Bell measurement on one of the EPR pair and |ψi. Then the remitter tells the outcome to the receiver via classical channel, by which the receiver can recover the information of |ψi by performing a unitary operation on the other EPR pair. Through this measurement, quantum states the remitter possessed are discarded and the coin |ψi is sent to the receiver.

In this way, the coin data dose not remain in remitter's hand and therefore this solves the double-spending problem. For successfully communicating the information of |ψi, we employ a quantum key distribution (QKD) protocol and the remitter and the receiver shear a private key. The most well-known is BB84. The remitter decodes the outcome of a Bell measurement and 4 tell it to a receiver via open channel. By decoding it, the receiver can get the coin.

Verification by use of quantum digital signature: qBitcoin is a quantum chain equipped with a transaction system. There a coin, which is a quantum state, is to be delivered and transactions are approved once if signature of coin's owner is verified. Security of modern digital signatures is based on the difficulty of solving a mathematical problem, such as finding the factors of large numbers (as used in the RSA algorithm). However, the task of solving these problems becomes feasible when a quantum computer is available. Moreover, traditional Bitcoin uses the classical coding, hence it is important to find an alternative way.

To fix this problem, quantum digital signature schemes, which is quantum mechanical digital signature, are in development to provide protection against tampering, even from parties in possession of quantum computers and using powerful quantum cheating strategies. We employ quantum digital signature for qBitcoin. The scheme proposed by Gottesman and Chuang is the most famous. It is essentially given by a quantum one-way function whose input k is a classical bit-string and output is a corresponding quantum state |fki and 5 inverting k is impossible thanks to quantum information theory

k → |fk easy
|fk→ k impossible

There is a key distribution method which secures the quantum digital signature which allows us to design qBitcoin on this scheme. Unlike Bitcoin, there is a limitation of issuing public keys of qBitcoin owners. If k has length L = O(2n), then one should make T copies of |fki so that L − nT 1 since if one observes too many copies of the public key, then a chance of successfully guessing the initial private key k becomes big, which is a consequence of Holevo's theorem. Therefore, we should limit the number of copies of any public key for the map k 7→ |fki being a quantum one-way function and such public keys are distributed to the corresponding number of other participants so that they can verify the signature.

The system of the quantum digital signature requires other participants to be involved in verifying the signature, hence it is naturally compatible with the concept of Bitcoin as a P2P electric cash system. Moreover, hash algorithm is not to be used and a transmitter must sign every single bit of a invoice. The procedure of a transaction is illustrated and described as follows:

1. A remitter and a receiver shear a private key using a QKD protocol, such as BB84.

2. Remittance is accepted if and only if a coin c = (r, |ψi) has the same serial numbers with respect to r and |ψi. 1 Practically, we may also convert a classical private key k into a quantum private key |ki and we consider a quantum one-way function |ki 7→ |fki. In this way the quantum private key |ki is secure since nobody else but the owner can copy it by virtue of the no-cloning theorem and since it is impossible to invert |ki from |fki.

3. The remitter encodes |ψi.

4. The remitter sends a remittance request which includes the record r, the signature s = (k, |fki) and the encoded information of |ψi to randomly chosen participants who are able to receive the corresponding public key |fki.

5. The receivers of the request verify the signature.

6. If the signature is approved, then one of the receivers renews the record and open it to public. (Some reward will be given to the one(s) for incentive.

7. The receiver of qBitcoin can receive the coin by decoding the information of c.

Security and Privacy

Here we mention the security of qBitcoin against several scenarios of cheaters. We first assume a remitter is a cheater. The case where the remitter copies a coin data and sends them more than two persons is already rejected since the remitter does not know the corresponding quantum state of a coin and so any copy of a coin cannot be generated. Moreover, no third party can steal a coin by virtue of security of a QKD protocol. Namely, for trying to steal a coin, a third party needs to wiretap communication between a remitter and a receiver and to get a private key sheared by them, however, this attempt never becomes successful in principle since a QKD should be protected by laws of physics.

qBitcoin strengths owner's privacy is better than Bitcoin. The risk of Bitcoin is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner. qBitcoin solves this point by using quantum digital signature of type proposed by Gottesman and Chuang. There owners' private keys are not secret and any key is not link to themselves. Moreover, owners can generate keys as many as they like, hence it is impossible even to guess to whom they belong.

In practice, it will be also important to consider how one who does not oppose a quantum computer can use quantum money since only a limited number of people will be able to have a first-generation quantum computer. In 7 this case, one who wants to trade quantum money will be forced to access to a quantum computer at an exchange. Here question is how to protect owner's privacy. Fortunately, we have a good solution to this issue. Namely, so called blind quantum computation[7,8] is a secure protocol which enables a client (Alice) without a quantum computer to delegate her quantum computation to a server (Bob) with a fully-fledged quantum technology in such a way that Bob cannot obtain any information about Alice's actual input, output and algorithm. This protocol is very secure and robust against realistic noise thanks to topological blind quantum computation.[9]

Applying this protocol to qBitcoin, owner's privacy should be perfectly protected. On the other hand, establishing classical blind computation in a practical manner is still open problem. That is to say, in the conventional Bitcoin, private information of coin owners is stored at market place and can be leaked out.

Related works

The attempt to making a money system based on quantum mechanics has a long history. It is believed that Wiesner made a prototype in about 1970, in which quantum money that can be verified by a bank is given. In his scheme, quantum money was secure in the sense that it cannot be copied due to the no-cloning theorem, however there were several problems. For example, a bank needs to maintain a giant data base to store a classical information of quantum money. Aaronson proposed a quantum money scheme where public key was used to verify a banknote and later his scheme was developed in. There is a survey on trying to quantize Bitcoin based on a classical blockchain system and a classical digital signature protocol.

However, all those works rely on classical digital signature protocols and classical coin transmission system, hence computational hardness assumptions are vital to their systems. In other words, if a computer equipped with ultimate computational ability appears someday, the money systems above are in danger of collapsing, as the bank systems today face.

Conclusion and Future Work

What we presented in this study can be summarized as follows. qBitcoin is a decentralized online quantum cash system and the significant change is that quantum states as coins are exchanged in addition to transaction descriptions. This secures traditional Bitcoin much better than previous good works in the following sense that no one can cheat transactions and no third party can steal any information illegally according to the laws of physics. Moreover, privacy of owners is perfectly protected. By virtue of the successful blind quantum computation, we also emphasize that one without full quantum technology can trade quantum money on qBitcoin without having to worry about any privacy problem. This is never achievable on Bitcoin. Furthermore, qBitcoin can complete a transaction faster than Bitcoin since a blockchain is replaced by a quantum chain.

Regarding future work, it will be interesting to invent a quantum blockchain, which accommodates quantum information and remittance requests are accepted by rigorous peer review. Straightforward implementation of a blockchain with quantum states is complicated by the fact that the original protocol is based on sending several copies of received messages to other participants. For instance, Alice sends Charlotte and David a message that she received from Bob. It is a nontrivial task due to the constraints of the no-cloning theorem.

Acknowledgement

I am thankful to Dr. Kumar Gautam for his guidance. Along with that I gained a lot of knowledge on computing and cyber security threats posing our technical infrastructure by

Mr. Lokesh Bhanduria, Deputy Director at Cybersecurity wing of National Technical Research Organization, Government of India.

References

1. https://arxiv.org/pdf/1710.10377.pdf

2. https://arxiv.org/pdf/1708.04955.pdf

3. https://www.rsaconference.com/writable/presentations/file_upload/fon4-t11_hacking_blockchain.pdf

4. https://mpra.ub.uni-muenchen.de/82832/1/MPRA_paper_82832.pdf

5. http://www.nexusearth.com/downloads/nexus-peer-peer.pdf

6. https://theqrl.org/whitepaper/QRL_whitepaper.pdf

7. https://www.r3.com/wp-content/uploads/2017/06/survey_confidentiality_privacy_R3.pdf

8. https://docbox.etsi.org/Workshop/2017/201709_ETSI_IQC_QUANTUMSAFE/TECHNICAL_TRACK/S03_THREATS/GHEORGHIU_IQC.pdf

9. http://www.silicon.co.uk/security/quantum-computing-security-bitcoin-221871?print=pdf.

(Received 25th October 2018, accepted 29th November 2018)