Quantum Information Processing (2020) 19:420
https://doi.org/10.1007/s11128-020-02915-y

A novel quantum blockchain scheme base on quantum entanglement and DPoS

Yu-Long Gao[1] · Xiu-Bo Chen[1,2] · Gang Xu[3] · Kai-Guo Yuan[1] · Wen Liu[4,5] · Yi-Xian Yang[1,2]

Received: 2 December 2019 / Accepted: 26 October 2020 / Published online: 17 November 2020

Abstract

In this paper, a novel quantum blockchain scheme is proposed to optimize the security of blockchain. Firstly, we propose the definition of quantum blockchain and provide its construction in detail. Additionally, its advantages are also summarized in this work. Secondly, based on the quantum no-cloning theorem, we define a new type of cryptocurrency which we call it quantum coin. Meanwhile, we adopt quantum entanglement and DPoS to design a novel quantum blockchain scheme. At last, we analyze the security of this proposed scheme in terms of the secret keys and quantum coin. It is shown that some attacks, such as man-in-the-middle attack, double spending attack and state-estimation attack, can be resisted. More specifically, under quantum computing attacks, the scheme is also secure. To sum up, through the principles of quantum cryptography and DPoS, this novel quantum blockchain obviously provides better security and higher efficiency.

Keywords Blockchain · Quantum cryptography · Bell state · Quantum entanglement · DPoS

✉ Xiu-Bo Chen
flyover100@163.com

[1] Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

[2] Guizhou Provincial Key Laboratory of Public Big Data, GuiZhou University, Guiyang 550025, Guizhou, China

[3] School of Information Science and Technology, North China University of Technology, Beijing 100144, China

[4] State Key Laboratory of Media Convergence and Communication, Communication University of China, Beijing, China

[5] School of Computer Science and Cybersecurity, Communication University of China, Beijing 100024, China

1 Introduction

In 2008, blockchain [1] was firstly described. In general, it is a new de-trusted, transparent and distributed ledger technology. In this new chain structure, every generated block has to include a cryptographic hash value of its previous block. Then, according to a certain consensus mechanism algorithms, such as proof of stake (PoS), delegated proof of stake (DPoS) and proof of work (PoW), the new generated block is agreed by all nodes in this distributed network. By this way, a continuously growing chain of blocks is generated. Subsequently, in 2014, by implementing smart contract, Ethereum blockchain [2, 3] was designed which is more practical than before. In general, smart contract provides a built-in fully fledged Turing-complete programming language for Ethereum blockchain, so that we can easily upload and execute contracts on the blockchain. By the way, it maximumly expands the potential application for blockchain technology. More importantly, cryptography algorithm plays a specifically important role in blockchain, for example elliptic curve cryptography (ECC) algorithm and SHA-256 algorithm. More exactly, they are closely related to not only blockchain's security and efficiency, but also the practical applications of blockchain.

However, with the development of quantum computing logarithm, these classical public key cryptography (PKC) algorithms are not secure any more. As is known to all, Shor presented some quantum algorithms [4] which can solve discrete logarithm problem and factoring integer problem. It means that the RSA [5], DSA and ECC algorithms [6, 7] cannot resist the quantum computing attacks. In particular, quantum computing attacks also can decrease the security of the underlying hash function. Afterward, Grover [8, 9] proposed a quantum mechanical algorithm which is regarded as an efficient method to find the preimage of a value for a function, even though it is the hash function. Obviously, blockchain technology whose security depends on the ECC algorithm and hash function is no longer secure [10]. This issue deserves our close attention and serious consideration.

At the same time, for the sake of resisting quantum computing attacks, quantum cryptography [11, 12] was proposed and discussed. As we know, based on the fundamental properties of quantum mechanics, such as Heisenberg uncertainty principle [13], quantum cryptography is different from conventional PKC and proven to be fundamentally secure. In 1984, the first quantum key distribution (QKD) protocol, also called BB84 protocol, was proposed [14] which was proven to be unconditional secure. Subsequently, because of its advantages, quantum cryptography has been paying more and more attention, including quantum key distribution [15–17], quantum secure direct communication (QSDC) [18, 19], quantum secret sharing (QSS) [20, 21], quantum digital signature(QDS) [22] and Quantum PKC [23].

Considering the unconditional security of quantum cryptography, we try to introduce principles of quantum mechanics into blockchain. In general, combining the quantum mechanics with blockchain, the study of quantum blockchain (QB) has become a hot research topic, since it is of great significance in dealing with the threat from quantum computing attacks. In 2016, Jonathan adopted the no-cloning theorem of quantum mechanics to introduce quantum bitcoin [24]. And he also simply constructed a quantum bitcoin protocol for transaction system. However, his scheme is rather inefficient. In 2018, the notion of quantum blockchain was proposed [25]. In this paper, Kiktenko used QKD protocol for information-theoretically secure authentication across an urban fiber network. Afterward, Rajan simply proposed a new conceptual design for a quantum blockchain [26]. And a new kind of innovative quantum blockchain with quantum entanglement in time was proposed in the Ref. [26]. Although this construction of quantum blockchain is very special, his work is still not complete. Some detailed algorithms and security analysis of his scheme are not provided in his paper. Furthermore, some other construction of combining blockchain with quantum has been presented either [27, 28]. As far as we see, the research on quantum blockchain is still less, and there are still many problems to be faced and studied.

Inspired by these above references, in this paper, we mainly study the security of blockchain and construct a novel full quantum blockchain base on Bell states. The main contributions of our research are summarized as follows.

- To begin with, we construct a novel full quantum blockchain. In this construction, we provide a new definition of quantum blockchain and describe its quantum information processing in detail. Additionally, its advantages are also summarized in this work.
- Based on the quantum no-cloning theorem, it is impossible to copy an arbitrary quantum state. Quantum mechanics provides an excellent basis on which to build a cryptocurrency and prevent double spending attack. Therefore, we define a new type of cryptocurrency, quantum coin. In particular, we propose a novel quantum blockchain scheme base on quantum entanglement and use this scheme to complete a transaction.
- We analyze the security of proposed scheme in terms of the secret keys and quantum coin. In these discussions, it shows that our scheme can resist some familiar attacks, such as double spending attack, man-in-the-middle attack and state-estimation attack. Our research can be regarded as a new construction for quantum blockchain which makes blockchain is secure under quantum computing attacks.

More exactly, in Sect. 2, we mainly introduce some quantum cryptography theorems and operation which are used in our scheme. In Sect. 3, we propose a novel quantum blockchain scheme base on quantum entanglement and DPoS. Then, we use this scheme to complete a transaction as an example. In Sect. 4, we analyze the security of our proposed quantum blockchain scheme. At last, some concluding remarks are given in Sect. 5.

2 Preliminaries

2.1 Quantum cryptography

Quantum cryptography is an interdisciplinary subject which combines cryptography and quantum mechanics, and it is an important research topic. The concept of quantum cryptography was put forward as early as 1960s. In 1984, the emergence of the first quantum key distribution protocol marked the advent of the era of quantum cryptography. Quantum cryptography includes quantum key distribution, quantum secure direct communication, quantum authentication, quantum signature and so on. At present, the quantum key distribution protocols mainly include BB84 protocol, B92 protocol and E91 protocol.

The theoretical basis of quantum cryptography is quantum mechanics, which uses physical principles to encrypt and protect information. For instance, quantum entanglement is a very significant role in quantum cryptography [29]. More importantly, the security of quantum cryptography is based on the following three basic principles of quantum mechanics: Heisenberg uncertainty principle, quantum no-cloning theorem [30, 31] and quantum collapse principle [32]. With many years of development, the traditional cryptography has been very mature. However, compared with quantum cryptography, the difference is significant, mainly in the following aspects.

(1) The traditional cryptography is generally based on a difficult mathematical problem, and its essence is limited by the current computing power. With the rapid development of quantum computing, the computing power has made a qualitative leap. It is only a matter of time before the traditional password is cracked, and the traditional cryptography's security is greatly threatened. On the contrary, quantum cryptography is based on quantum mechanics, through physical principles rather than mathematical problems, so quantum cryptography is more secure.

(2) In traditional cryptography, it is difficult to prove that the key has not been stolen or changed by the eavesdropper in the process of transmission and distribution. In contrast, quantum cryptography can effectively identify the existence of attackers in the process of key distribution, so as to ensure the security of communication process.

2.2 Rajan's quantum blockchain

In Ref. [26], Rajan proposed a conceptual design for a quantum blockchain using entanglement in time. The specific process of the scheme is as follows. At first, in the coding process, each block with records is converted to a temporal Bell state generated at a specific time as follows.

$$\left|\beta_{r_1r_2}\right\rangle^{0,t} = \frac{1}{\sqrt{2}}\left(\left|0^0\right\rangle\left|r_2^t\right\rangle + (-1)^{r_1}\left|1^0\right\rangle\left|\overline{r_2}^t\right\rangle\right),$$

where $\bar{r}_2$ is the negation of r_2. In addition, the superscripts in keys indicate the time of photon absorption. Thus, just like blockchain technology, this conversion implements a method to make time stamps for each quantum block.

As described earlier, in this scheme, the system generates many temporary Bell states. Subsequently, they are absorbed at their own time, respectively. At last, we get the following blocks for recording data,

$$\left|\beta_{r_1r_2}\right\rangle^{0,t}, \left|\beta_{r_3r_4}\right\rangle^{t,2t}, \left|\beta_{r_5r_6}\right\rangle^{2t,3t}.$$

In particular, by using the fusion approach, these temporal Bell states can be projected into the growing temporal GHZ (Greenberger–Horne–Zeilinger) state. Thus, in his scheme, the system strings the bits of the clock state in time sequence. Therefore, quantum blockchain is programmed into a temporal GHZ state of photons as follows,

$$\left|\mathrm{GHZ}_{r_1 r_2 \cdots r_{2n}}\right\rangle^{0,t,t,2t,2t,\ldots,(n-2)t,(n-1)t,(n-i)t,nt} = \frac{1}{\sqrt{2}}\left(\left|0^0 r_2^t \cdots r_{2n}^{nt}\right\rangle + (-1)^{r_1}\left|1^0 \overline{r}_2^t \cdots \overline{r}_{2n}^{nt}\right\rangle\right).$$

Here the subscripts refer to the concatenated string of all the blocks, and the superscripts denote timestamps. The timestamp allows the bit string of each block to be distinguished from the binary representation of the temporal GHZ base state. We can see from the above equation, by using the quantum entanglement in time, the first quantum block $\left|\beta_{r_1 r_2}\right\rangle^{0,\,t}$ and the second quantum block $\left|\beta_{r_3 r_4}\right\rangle^{t,\,2t}$ can be generated in turn. Thus, this quantum system creates a linking of quantum blocks.

3 Quantum blockchain

3.1 Quantum internet

Quantum Internet [33–35] refers to the whole system which includes many kinds of packet switching quantum and classical networks. In the network graph structure, quantum network is a sub-network of classical network, whose hosts and routers have the ability to process quantum information. There are not only classical channel connections between these nodes to transmit classical information, but also quantum channel connections to transmit quantum information.

In order to realize the future network system based on quantum Internet, we need to establish a unified protocol to support quantum information transmission. This opinion is also raised in Wehner's prospective paper on quantum network technology route which is published on Science in 2018 [36]. Unlike classical network data, which can be read, written and duplicated, the quantum mechanical properties of quantum network data (entanglement, measurement, non-cloning, etc.) make the establishment of quantum network protocols challenging. As Kimble pointed out [33], quantum interconnection can convert quantum states from one physical system to another physical system in a reversible fashion. Meanwhile, optical interactions of single photons and atoms can be used to realize quantum connectivity in a quantum network. Thus, based on the quantum principles of entanglement distribution and quantum teleportation, quantum networks with many nodes and channels can be realized.

Generally speaking, the foundation of realizing blockchain technology cannot be separated from a distributed network as a technology platform. In this way, each node in this distributed network can agree on the same public ledger through consensus mechanism in time. At present, the research of quantum network is still a relatively new topic, which involves many related fields such as quantum computing, quantum communication and so on. It is an exciting frontier of knowledge and technology and provides a new direction for quantum research. In this paper, assuming that through existing technologies, we have implemented a distributed interconnected quantum network.

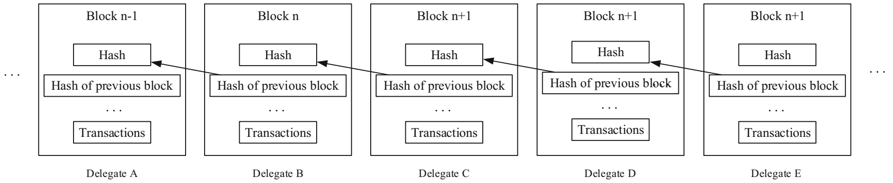

Fig. 1 Blocks based on DPoS

3.2 Delegated proof of stake

Under the environment of quantum computing, obviously, using computing power as consensus mechanism to compete for the next block, such as PoW, is not suitable for quantum blockchain. Therefore, we need to choose a kind of consensus mechanism, such as Delegated Proof of Stake (DPoS), which does not take computing power as the decisive factor and can keep a fair method in blockchain. DPoS is a new scheme to ensure the security of cryptocurrency network. It not only solves the problems of PoW and PoS, but also counteracts the negative effects of centralization by implementing fair democracy.

Generally speaking, as shown in Fig. 1, DPoS allows block producers, such as delegate A, delegate B, delegate C and so on, to take turns generating the next block every 3 s, and others have been scheduled for subsequent processes. If there is no delegate misses his order, the chain they produced is bound to be the longest. On the contrary, block delegate who produce blocks at unspecified times, these blocks are considered invalid.

Although both PoW and PoS can effectively solve the problem of accounting consistency and consensus, the existing bitcoin PoW is purely dependent on computing power, which makes the group of miners who are specialized in mining seem to be completely separated from bitcoin community, and the huge computing power of some mining pools seems to be another center, which conflicts with the thought of bitcoin decentralization. Although PoS takes into account the shortage of PoW, however, the choice based on the equity balance will lead to the excessive power of the account of the richest person, which may dominate the bookkeeping power.

The emergence of DPoS is just to solve the above problems of PoW and PoS. Different from PoW and PoS, DPoS is a consensus algorithm based on voting, which will never appear the phenomenon of computing power monopoly. The advantage is that it shortens the time to reach consensus. In addition, because of the voting mechanism, there is no need to consume a lot of energy for mining.

3.3 Constructing quantum blockchain

Inspired by the Ref. [26], in this subsection, we try to construct a novel full quantum blockchain. In this construction, we use quantum entanglement in time to link these quantum blocks. As shown in Fig. 2, by using the quantum entanglement in time, the $n-1$th quantum block $\left|\beta_{r_{2n-3}r_{2n-2}}\right\rangle^{(n-2)t,\,(n-1)t}$ and the nth quantum block

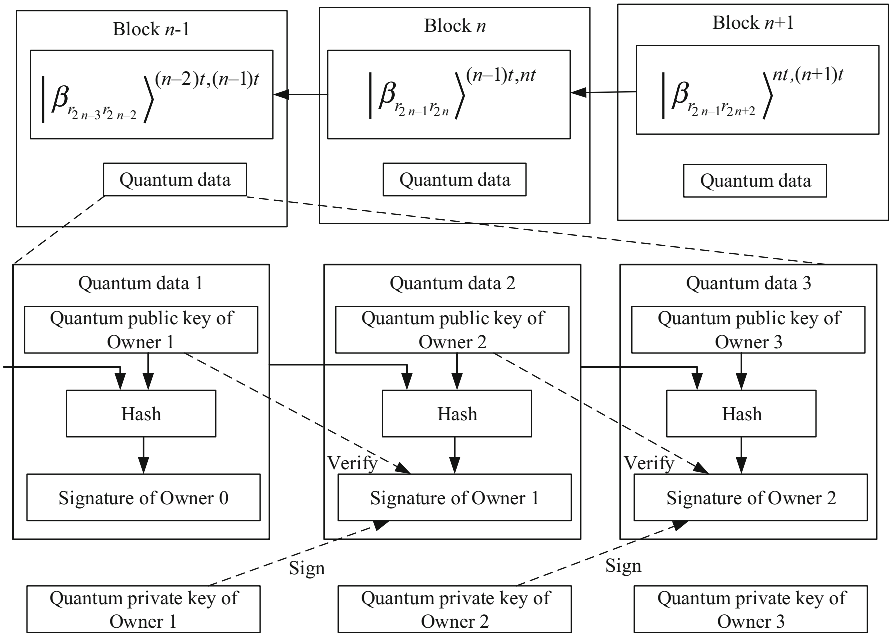
Block n-1
$\left|\beta_{r_{2n-3}r_{2n-2}}\right\rangle^{(n-2)t,(n-1)t}$
Quantum data
Block n
$\left|\beta_{r_{2n-1}r_{2n}}\right\rangle^{(n-1)t,nt}$
Quantum data
Block n+1
$\left|\beta_{r_{2n-1}r_{2n+2}}\right\rangle^{nt,(n+1)t}$
Quantum data
Quantum data 1
Quantum public key of Owner 1
Hash
Signature of Owner 0
Quantum data 2
Quantum public key of Owner 2
Hash
Verify
Signature of Owner 1
Quantum data 3
Quantum public key of Owner 3
Hash
Verify
Signature of Owner 2
Sign
Sign
Quantum private key of Owner 1
Quantum private key of Owner 2
Quantum private key of Owner 3

Fig. 2 Organization structure of quantum blockchain

$\left|\beta_{r_{2n-1}r_{2n}}\right\rangle^{(n-1)t,\,nt}$ can be generated in turn and linked. Then, in these quantum blocks, we need to store useful quantum data. At the same time, these quantum data need to be guaranteed to be verifiable and unforgeable. Therefore, we propose a quantum information authentication based on Bell states and introduce it into blockchain technology. More specifically, based on the fundamental properties of quantum mechanics and quantum cryptography, these distributed nodes share an authenticated and secure quantum information database through quantum network. Each user can generate a verifiable quantum information through quantum signatures, which is published in quantum networks and verified by other nodes. Then, other nodes compete for new quantum blocks through a fair consensus and link these quantum blocks by quantum entanglement in time. At last, all nodes add this new quantum block to their own quantum blockchain through quantum channels.

Generally speaking, we consider that quantum blockchain needs to be satisfied with these following characteristics: (1) decentralized structure, (2) a distributed interconnected quantum network, (3) in this quantum network, each node has quantum capabilities, including quantum storage, quantum preparation, quantum transmission and other functions, (4) open and transparent information and (5) consensus on a common quantum database.

Definition 1 *Quantum blockchain* Quantum blockchain mainly consists of six steps as follows: *key generation*, *encryption*, *published*, *decryption*, *mint* and *linking*.

Initialization In order to create an ideal quantum design, the quantum blockchain system should string the bits of Bell state in order through an entanglement in time.

Key generation Suppose there is a trusted QB system which is used for authenticating each user's identity. It runs key generation algorithm to generate a pair of quantum public and private secret key (pk, sk) for each user.

Encryption Sender runs encryption algorithm to encrypt quantum coin $|\varphi\rangle$ with receiver's public key pk_r and outputs a cipher qubit sequence $c = \mathrm{encryption}(\mathrm{pk}_r, |\varphi\rangle)$. In particular, he also needs to generate a quantum signature e with his private key pk_s.

Published The QB system sends the quantum coin to receiver's address, and then, sender generates and publishes transaction information in the quantum network.

Decryption Sender securely sends the cipher qubit sequence $c = \mathrm{encryption}(\mathrm{pk}_r, |\varphi\rangle)$ and quantum signature e to receiver. Then, receiver runs decryption algorithm to obtain the quantum coin and verify this signature. If the conditions are satisfied, it means that this quantum coin is available and this signature is generated by sender. Otherwise this output is rejected.

Verification Delegates verify the signature's correctness. If the above conditions are satisfied, the transaction is included in a new quantum block. Otherwise, this transaction is rejected.

Linking Through the consensus mechanism, nodes compete for a new quantum block. Then, all nodes add this new quantum block to their own quantum blockchain. Thus, the stored data in the whole network nodes can reach a consensus.

Compared with the current blockchain technology, we summarize four special advantages of quantum blockchain as follows.

- Based on the principle of quantum non-cloning, quantum states cannot be duplicated, which is significance to the financial transactions based on our designed quantum blockchain. In the case of quantum states which is regarded as cryptocurrency, the advantages will be highlighted. Quantum coin cannot be forged and duplicated, which makes it innate and unconditional resistance to double spending attack.
- Each user transmits information with the qubit for communication through quantum channel. Due to the quantum superdense coding, in these quantum networks, information transmission will be more efficient.
- Confirming an information in quantum blockchain will be much faster than current blockchain technology. (The time takes averages on 1 h.) Especially in trading, it means that the quantum blockchain-based quantum trading confirmation will be very fast, just like a face-to-face transaction.
- Compared to blockchain, quantum blockchain is more secure. Combining with quantum cryptography and principles of quantum, quantum blockchain provides strong security for users which can resist quantum computing attacks. Obviously, QB is more secure than current blockchain technology. Especially in applications of economics, such as finance and credit, quantum blockchain has great advantages.

3.4 Quantum blockchain scheme base on Bell states

The proposed quantum blockchain was described in Sect. 3.3. Here, we will propose a novel quantum blockchain scheme base on Bell states and use it to complete a transaction between two users. Firstly, we need to provide a definition for quantum coin.

Definition 2 *Quantum coin* All of quantum coins are generated and distributed by the QB system when they are be transmitted for the first time. Quantum coin is just a qubit sequences which is transmitted by quantum channel in our scheme (ex. n-qubit denotes a quantum coin). In this paper, we present a new quantum cryptocurrency scheme based on quantum blockchain. According to the quantum no-cloning theorem, it is impossible to copy an arbitrary quantum state (quantum coin). So quantum mechanics provides obvious advantages for quantum state which is regarded as a cryptocurrency, and this new type of cryptocurrency can prevent double spending attack. It shows that quantum coin are secure against counterfeiting.

Suppose that there is a trusted quantum blockchain system. Now, without loss of generality, Alice and Bob are regarded as two users who are trading through quantum cryptocurrency scheme based on QB, and Alice transfers her quantum coin to Bob. The steps are shown as follows in detail.

Step 1 Initialization In order to create an ideal quantum design, according to the following formula, the quantum blockchain system should string the bits of Bell state in order through an entanglement in time.

$$\left|\mathrm{GHZ}_{r_1 r_2 \cdots r_{2n}}\right\rangle^{0,t,t,2t,2t,\ldots,(n-2)t,(n-1)t,(n-i)t,nt} = \frac{1}{\sqrt{2}}\left(\left|0^0 r_2^t \cdots r_{2n}^{nt}\right\rangle + (-1)^{r_1}\left|1^0 \overline{r}_2^t \cdots \overline{r}_{2n}^{nt}\right\rangle\right).$$

Thus, for example, the first three blocks are $|\beta_{00}\rangle^{0,\,t}$, $|\beta_{10}\rangle^{t,\,2t}$ and $|\beta_{11}\rangle^{2t,3t}$ in time, respectively. Thus, this quantum blockchain $|\mathrm{GHZ}_{001011}\rangle^{0,\,t,\,t,\,2t,\,2t,\,3t}$ is produced by system. Assume that the latest stored block currently is $\left|\beta_{r_{2n-3} r_{2n-2}}\right\rangle^{(n-2)t,\,(n-1)t}$.

Step 2 Key generation QB system generates a pair of quantum key for each user, i.e., Alice and Bob. Without loss of generality, consider Alice as our example. The particular process is as follows.

(1) QB system prepares a sequence of qubit pairs $\{(A_{p1}, A_{s1}), (A_{p2}, A_{s2}), \ldots, (A_{pn}, A_{sn})\}$. Each pair is in the Bell state

$$\left|\psi^+\right\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{1}$$

The two qubit sequences $A_p = \{A_{p1}, A_{p2}, \ldots, A_{pn}\}$ and $A_s = \{A_{s1}, A_{s2}, \ldots A_{sn}\}$ are Alice's master public key and master private key, respectively. Similarly, QB system also generates a pair of quantum key for Bob, which the master public key and master private key are $B_p = \{B_{p1}, B_{p2}, \ldots, B_{pn}\}$ and $B_s = \{B_{s1}, B_{s2}, \ldots B_{sn}\}$, respectively.

(2) QB system randomly and uniformly selects two qubit sequences A_p^1 (public key) from $A_p = \{A_{p1}, A_{p2}, \ldots, A_{pn}\}$ and A_s^1 (private key) from $A_s = \{A_{s1}, A_{s2}, \ldots A_{sn}\}$ for Alice, respectively. Similarly, QB system can random select securely two qubit sequences B_p^1 (public key) from $B_p =$

$\{B_{p1}, B_{p2}, \ldots, B_{pn}\}$ and B_s^1 (private key) from $B_s = \{B_{s1}, B_{s2}, \ldots, B_{sn}\}$ for Bob.

(3) Based on the BB84 protocol, QB system random transmits Alice's private key A_s^1 and Bob's public key B_p^1 to Alice by using a certain quantity of decoy states. Correspondingly, QB system also securely transmits Bob's private key B_s^1 and Alice's public key A_p^1 to Bob as the same way.

Step 3 Encryption Suppose there is an x-qubit quantum coin $m = \{m_1, m_2, \ldots, m_x\} \in \mathbb{Z}_2$ which Alice wants send to Bob. Alice encrypts this quantum coin m with Bob's public key and generates a new quantum transaction (m, h) as the following steps.

(1) Bob transmits his address q to Alice.
(2) Alice calculates the hash vale $h = \text{hash}(m)$ of this message and obtains a y-bit hash message $h = \{h_1, h_2, \ldots, h_y\} \in \mathbb{Z}_2$.
(3) Alice prepares an x-qubit sequence $a = \{a_1, a_2, \ldots, a_x\}$ with states $\{|m_1\rangle, |m_2\rangle, \ldots, |m_x\rangle\}$, respectively. Similarly, she can also generates a y-qubit sequence $s = \{s_1, s_2, \ldots, s_y\}$ with states $\{|h_1\rangle, |h_2\rangle, \ldots, |h_x\rangle\}$, respectively.
(4) Alice encrypts her message m and its hash value h with Bob's first x qubits of public key B_p^1 and first y qubits of her private key A_s^1 via a CNOT operation. That is

$$C_{B_{Pi}a_i}|\psi\rangle_{B_{pi}B_{si}}|m_i\rangle_{a_i} = \frac{(|00m_i\rangle + |11\overline{m_i}\rangle)_{B_{pi}B_{si}a_i}}{\sqrt{2}}, \tag{2}$$

$$C_{A_{si}s_i}|\psi\rangle_{A_{pi}A_{si}}|h_i\rangle_{s_i} = \frac{\left(|00h_i\rangle + \left|11\overline{h_i}\right\rangle\right)_{A_{pi}A_{si}s_i}}{\sqrt{2}}, \tag{3}$$

where $\overline{m_i} = 1 - m_i$ and $\overline{h_i} = 1 - h_i$.

Step 4 Published The system automatically verifies and splits this quantum transaction (q, A_p^1, m, h), and it sends the quantum coin m and signature h to Bob's address. Then, the remaining transaction information combination (q, A_p^1, h) is published in the quantum network.

Step 5 Decryption Bob recovers the qubit sequences with his private quantum key. Then, he confirms this message is sent by Alice and obtains quantum coin by the following steps.

(1) Bob performs a CNOT operation, and then, he uses his private key B_s^1 and Alice's public key A_p^1 to, respectively, decrypt these two qubit sequences

$$C_{B_{si}a_i}\frac{(|00m_i\rangle + |11\overline{m_i}\rangle)_{B_{pi}B_{si}a_i}}{\sqrt{2}} = |\psi\rangle_{B_{pi}B_{si}}|m_i\rangle_{a_i}, \tag{4}$$

$$C_{A_{pi}s_i}\frac{\left(|00h_i\rangle + \left|11\overline{h_i}\right\rangle\right)_{A_{pi}A_{si}s_i}}{\sqrt{2}} = |\psi\rangle_{A_{pi}A_{si}}|h_i\rangle_{s_i}. \tag{5}$$

Then, Bob obtains a new quantum coin m' and a new hash quantum signature h'.

(2) Bob verifies $h'' = \text{hasn}(m')$ and $h' = h''$. If the above equations are satisfied, it means that the quantum coin is complete and signature is the generated by Alice, otherwise this output is rejected.

Step 6 Verification Delegates verify the correctness of this signature for the sake of confirming whether this transaction is generated by Alice. If the above conditions are satisfied, this transaction information combination (q, A_p^1, h) will be included in a new quantum block. Otherwise, this transaction will be rejected.

Step 7 Linking Through DPoS, the delegates generate the next block in turn every three seconds in the specified order. Suppose the next block producer selected by voting is delegate Alice. So delegate Alice generates the next new quantum block $\left|\beta_{r_{2n-1}r_{2n}}\right\rangle^{(n-1)t,\,nt}$ and links this new quantum block by quantum entanglement in time. Alice will also be rewarded by the system. At last, all nodes add this new quantum block to their own quantum blockchain through quantum channels.

4 Security analysis

Currently, cryptography plays a very fundamental role in blockchain, and its security is based on the intractability of elliptic curve discrete logarithm problem. However, with the development of quantum computing, quantum computer can have powerful parallel computing ability which becomes a great threat to conventional cryptographic algorithms, especially ECC logarithm. It has become a tendency to research quantum blockchain for dealing with this new challenge. Therefore, in this paper, we mainly study the security of blockchain and construct a novel full quantum blockchain.

In this section, we will analyze the security of our proposed scheme. It includes the security of secret keys and quantum coin. In these analyses, some attacks, such as forgery attack, man-in-the-middle attack and state-estimation attack, are also considered.

4.1 Security of secret keys

In quantum blockchain, quantum public key is generated by quantum blockchain system through randomly selecting a qubit sequences A_p^1 from her master public key A_p. In this stage of quantum key distribution, BB84 protocol provides us with unconditional security for secret key. Meanwhile, because of this quantum blockchain system is trusted, user's public key is secure and identity can be convinced. Furthermore, quantum blockchain system helps the sender and receiver to exchange their public keys each other, and the authentication process for user can resist forgery attack and man-in-the-middle attack.

Quantum private key is very important in quantum blockchain, which cannot be obtained by others. With the private key, the quantum data in quantum block can be verified to be authentic and credible. As we constructed, quantum blockchain system is trusted which can authenticate each user's identity. Without loss of generality, quantum blockchain system randomly and uniformly selects a qubit sequences B_s^1 from Bob's master private key B_s. Both the decoy states and private key states are in the same state, the maximally mixed state $\rho = \frac{|0\rangle\langle 0|+|1\rangle\langle 1|}{2}$. Therefore, no one can distinguish between these two states by measuring, that is, attacks on private keys will inevitably lead to changes in decoy states, and quantum state attacks will be discovered. In this stage, BB84 protocol provides us with unconditional security when QB system transmits B_s^1(Bob's private key) to Bob. Subsequently, when Bob wants to use his private key again with other user, he can obtain a new private key B_s^2 from the quantum blockchain system. Similarly, his public key is also updated. More exactly, each public–private key pairs will be used only once in the encryption stage. Through the one-time pad method and quantum no-cloning theorem, our proposed scheme can carry out unconditionally secure communications. Eventually, this flexible method makes secret keys different in each time. Therefore, the secret key is secure in our scheme.

4.2 Security of quantum coin

As our described, all of quantum coins are generated and distributed from the quantum blockchain system when they are be transmitted for the first time. In the step 3 *published*, quantum blockchain system automatically verifies and splits this quantum transaction. The quantum coin will be verified. If they are not generated by quantum blockchain system, this transaction will be objected. In particular, due to the no-cloning theorem of quantum mechanics, the quantum coin cannot be duplicated, thereby preventing counterfeiting in itself. Double spending attack can also be resisted in this quantum cryptocurrency scheme.

At the same time, there two ciphertext qubits that are sent to Bob by Alice. One is the quantum coin, and the other one is Alice's quantum signature. Both of the secret keys which are used to generate these ciphertext qubits are Bell states $\left|\psi^+\right\rangle = (|00\rangle + |11\rangle)\Big/\sqrt{2}$. Therefore, we can calculate that these two ciphertext qubits are in the same state. Furthermore, the attacker cannot get any information from these qubits. In particular, by using the decoy states in communication, any attack on these two ciphertext qubits will be detected.

More concretely, based on the fundamental properties of quantum mechanics, such as quantum no-cloning theorem and Heisenberg uncertainty principle, quantum coin is fundamentally secure, and attacker cannot obtain any useful information from these qubits. And the process of eavesdropping detection is introduced into it for the sake of guaranteeing its security. So the proposed scheme can resist state-estimation attack. More importantly, this flexible method which generates user's secret keys to encrypt plaintext is similar to one-time pad. Based on this way and quantum no-cloning theorem, the used secret keys are changed in each time. More importantly, based on quantum no-cloning theorem, it is impossible for attacker to copy an arbitrary quantum coin. Obviously, quantum mechanics provides obvious advantages for quantum coin. Therefore, this new type of cryptocurrency, quantum coin, can prevent double spending attack in quantum blockchain. To sum up, it shows that quantum coin is secure against counterfeiting. And quantum coin has better secure performance in our cryptocurrency scheme based on quantum blockchain, which cannot be decrypted without the corresponding private key.

4.3 Resistance to quantum computing attacks

As described in the previous sections, the user's private key has to be absolutely secure in blockchain technology. Unfortunately, under the environment of quantum computing, the traditional classical cryptography algorithm is no longer secure. For example, ECDSA algorithm, which is used to generate public–private key pairs for users in blockchain technology, has been proved to be completely cracked through quantum computing attacks. Therefore, with the development of quantum computing, current signature algorithm is difficult to satisfy blockchain's security needs.

In this paper, our quantum blockchain scheme is secure under quantum computing attacks for these following reasons. Firstly, quantum cryptography is a part of quantum information science. Different from the traditional cryptographic algorithm, it is a new cryptography based on the fundamental properties of quantum mechanics, which is proven to be fundamentally secure. Therefore, we propose a new quantum signature algorithm and introduce it into our quantum blockchain scheme to improve its security. Secondly, as mentioned above, each user can randomly generate his own quantum public–private key pair in this quantum blockchain scheme. And these used secret keys are changed in each time. Furthermore, in the stage of quantum key distribution, BB84 protocol provides us with unconditional security for secret keys. Meanwhile, any attacks on user's secret keys will inevitably lead to changes in decoy states. Thus, quantum state attacks will be discovered immediately. We have analyzed and proved the security of quantum secret keys and quantum coin in the previous subsections. Last but not least, the superposition principle of states in quantum mechanics makes the state of quantum information unit in a variety of possible superposition states, which makes quantum computing have strong computing power. Consequently, quantum computing attack can decrypt the traditional cryptography algorithm by solving some mathematical problems. However, the security of our quantum blockchain scheme is guaranteed by the principles of quantum mechanics, such as quantum no-cloning theorem and Heisenberg uncertainty principle. Therefore, the quantum computing attacks cannot obtain anything through calculation. To sum up, the proposed quantum blockchain scheme is secure under quantum computing attacks.

5 Conclusion

In this work, we present major security issues for blockchain and try to construct a novel quantum blockchain scheme to improve its security under the quantum computing attacks. It provides us with an open, public, decentralized ledger in a distributed network, which can be applied to many promising applications. Since it was put forward, blockchain has been widely concerned and studied. Nevertheless, it also exists some defects that cannot be ignored.

With the increasing potential use space of blockchain technology, the research on blockchain's security is of great significance to its application in the future. In this work, we mainly study the security of blockchain and construct a novel full quantum blockchain. Inspired by Ref. [26], we construct a novel full quantum blockchain. Then, we provide a secure cryptocurrency scheme based on our proposed quantum blockchain. Furthermore, we use it to complete a transaction with a new type of cryptocurrency (quantum coin) in this quantum blockchain. At last, we discuss the security of proposed scheme in terms of the secret keys and quantum coin. In these discussions, it shows that some attacks, such as double spending attack, man-in-the-middle attack and state-estimation attack, can be resisted. By using DPoS, the proposed scheme in this paper greatly shortens the time to reach a transaction and improves the efficiency. At the same time, because of the voting mechanism, the scheme does not need to consume a lot of energy for mining. Obviously, our research can be regarded as a new thought of quantum blockchain which makes blockchain is secure under quantum computing attacks. And it is also more efficient. The theoretical research results in this paper provide scientific basis for the future practicality. In summary, this novel quantum blockchain provides better security and higher efficiency for the development of blockchain in the future.

Acknowledgements This work is supported by the NSFC (Grant Nos. 61671087, 61962009), the Open Foundation of Guizhou Provincial Key Laboratory of Public Big Data (Grant Nos. 2018BDKFJJ018, 2019BDKFJJ010, 2019BDKFJJ014), the Open Research Project of the State Key Laboratory of Media Convergence and Communication, Communication University of China, China (Grant No. SKLMCC2020KF006), the BUPT Excellent Ph.D. Students Foundation (Grant No. CX2019232), the High-quality and Cutting-edge Disciplines Construction Project for Universities in Beijing (Internet Information, Communication University of China) and the Fundamental Research Funds for the Central Universities (Grant No. 2019XD-A02).

References

1. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008). https://bitcoin.org/bitcoin.pdf
2. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger. Ethereum Proj Yellow Pap **151**, 1–32 (2014)
3. Atzei, N., Bartoletti, M., Cimoli, T.: A survey of attacks on ethereum smart contracts (sok). In: International Conference on Principles of Security and Trust, pp. 164–186. Springer, Berlin, Heidelberg (2017)
4. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Foundations of Computer Science, 1994 Proceedings, 35th Annual Symposium on. IEEE, Santa Fe, NM, USA (1994)
5. Rivest, R.L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **26**(2), 96–99 (1978)
6. Miller V.S.: Use of elliptic curves in cryptography. In: Conference on the Theory and Application of Cryptographic Techniques, pp. 417–426. Springer, Berlin, Heidelberg (1985)
7. Koblitz, N.: Elliptic curve cryptosystems. Math. Comput. **48**(177), 203–209 (1987)
8. Grover L.K.: A fast quantum mechanical algorithm for estimating the median. In: Twenty-Eighth ACM Symposium on Theory of Computing. ACM (1996)
9. Grover, L.K.: Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett. **79**(2), 325 (1997)
10. Fedorov, A.K., Kiktenko, E.O., Lvovsky, A.I.: Quantum computers put blockchain security at risk. Nature **563**, 465–467 (2018)
11. Gisin, N., Ribordy, G., Tittel, W., et al.: Quantum cryptography. Rev. Mod. Phys. **74**(1), 145–195 (2001)

12. Yin, J., Li, Y.-H., Liao, S.-K., et al.: Entanglement-based secure quantum cryptography over 1,120 kilometres. Nature **582**(7813), 501–505 (2020)
13. Busch, P., Heinonen, T., Lahti, P.: Heisenberg's uncertainty principle. Phys. Rep. **452**(6), 155–176 (2007)
14. Bennett, C.H., Brassard, G.: An Update on quantum cryptography. In: Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19–22, 1984, Proceedings DBLP, pp. 475–480 (1984)
15. Grosshans, F., Van Assche, G., Wenger, J., et al.: Quantum key distribution using gaussian-modulated coherent states. Nature **421**(6920), 238 (2003)
16. Deng, F.G., Long, G.L.: Bidirectional quantum key distribution protocol with practical faint laser pulses. Phys. Rev. A **70**(1), 012311 (2004)
17. Lucamarini, M., Yuan, Z.L., Dynes, J.F., et al.: Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature **557**(7705), 400 (2018)
18. Wang, C., Deng, F.G., Li, Y.S., et al.: Quantum secure direct communication with high-dimension quantum superdense coding. Phys. Rev. A **71**(4), 044305 (2005)
19. Qin, H., Tang, W.K.S., Tso, R.: Establishing rational networking using the DL04 quantum secure direct communication protocol. Quantum Inf. Process. **17**(6), 152 (2018)
20. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**(3), 1829 (1999)
21. Xiao, L., Long, G.L., Deng, F.G., et al.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A **69**(5), 052307 (2004)
22. Liu, F., Qin, S.J., Su, Q.: An arbitrated quantum signature scheme with fast signing and verifying. Quantum Inf. Process. **13**(2), 491–502 (2014)
23. Nikolopoulos, G.M.: Applications of single-qubit rotations in quantum public-key cryptography. Phys. Rev. A **77**(3), 032348 (2008)
24. Jogenfors, J.: Quantum bitcoin: an anonymous and distributed currency secured by the no-cloning theorem of quantum mechanics (2016). arXiv:1604.01383
25. Kiktenko, E.O., Pozhar, N.O., Anufriev, M.N., et al.: Quantum-secured blockchain. Quantum. Sci. Technol. **3**(3), 035004 (2018)
26. Rajan, D., Visser, M.: Quantum blockchain using entanglement in time. Quantum Rep. **1**(1), 3–11 (2019)
27. Behera, A., Paul, G.: Quantum to classical one way function and its applications in quantum money authentication. Quantum Inf. Process. **17**(8), 200 (2018)
28. Tessler, L., Byrnes, T.: Bitcoin and quantum computing. Social Science Electronic Publishing, Rochester (2018)
29. Vedral, V.: Quantum entanglement. Nat. Phys. **10**(4), 256–258 (2014)
30. Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned. Nature **299**(5886), 802–803 (1982)
31. Dieks, D.: Communication by EPR devices. Phys. Lett. A **92**(6), 271–272 (1982)
32. Chernyak, V., Mukamel, S.: Effect of quantum collapse on the distribution of work in driven single molecules. Phys. Rev. Lett. **93**(4), 048302 (2004)
33. Kimble, H.J.: The quantum internet. Nature **453**(7198), 1023 (2008)
34. Gyongyosi, L., Imre, S.: Entanglement-gradient routing for quantum networks. Sci. Rep. **7**(1), 14255 (2017)
35. Gyongyosi, L., Sandor, I., Hung, V.N.: A survey on quantum channel capacities. IEEE Commun. Surv. Tutor. **20**(2), 1149–1205 (2018)
36. Wehner, S., David, E., Ronald, H.: Quantum internet: a vision for the road ahead. Science **362**(6412), eaam9288 (2018)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.