mathematics

MDPI

Article

Blockchain Consensus Mechanism Based on Quantum Teleportation

Xiaojun Wen [1], Yongzhi Chen [2,*], Wei Zhang [2], Zoe L. Jiang [3] and Junbin Fang [4]

[1] College of Computer Engineering, Shenzhen Polytechnic, Shenzhen 518055, China; wxjun@szpt.edu.cn
[2] College of Physics, College of Mechanical and Electrical Engineering, Shijiazhuang University, Shijiazhuang 050035, China; 1102078@sjzc.edu.cn
[3] College of Computer Science and Technology, Harbin Institute of Technology, Shenzhen 518055, China; zoeljiang@hit.edu.cn
[4] Department of Optoelectronic Engineering, Jinan University, Guangzhou 510632, China; tjunbinfang@jnu.edu.cn
* Correspondence: 1102052@sjzc.edu.cn

Abstract: The consensus mechanism is the core secret of the blockchain network. However, the consensus mechanism of the classical blockchain is based on the classical cryptosystem, which is based on the problem of computational complexity. With the improvement of computing power, the security of this cryptosystem is being threatened. In addition, the consensus mechanism of classic blockchain also has the following disadvantages: serious waste of computing resources and energy; the inability to withstand a 51% attack; low system throughput and large delay. Based on quantum teleportation technology and the randomness of quantum measurement, a consensus mechanism for a quantum blockchain system is proposed. Based on the physical properties of quantum mechanics, this scheme has the unconditional security of quantum cryptography. This new consensus mechanism does not involve a great deal of computing resources and hence has a lower energy consumption, shorter time delay and higher throughput. Furthermore, the new consensus mechanism could withstand a 51% attack.

Keywords: blockchain; consensus mechanism; quantum teleportation; quantum measurement

MSC: 81P94

check for updates

Citation: Wen, X.; Chen, Y.; Zhang, W.; Jiang, Z.L.; Fang, J. Blockchain Consensus Mechanism Based on Quantum Teleportation. *Mathematics* **2022**, *10*, 2385. https://doi.org/10.3390/math10142385

Academic Editor: Zongwei Luo

Received: 23 April 2022
Accepted: 20 June 2022
Published: 7 July 2022

1. Introduction

Blockchain, which is a strategic and prospective emerging technology, and an important cornerstone of the transformation from the information Internet to the value Internet, will bring profound reforms to economic and social development in the digital era. The applications of blockchain technology have extended into digital finance, the Internet of Things, intelligent manufacturing, supply chain management, digital asset trading and other fields [1–7]. At present, major countries in the world are accelerating the development of blockchain technology.

In a narrow sense, blockchain is a Distributed Database (or Distributed Ledger Technology, DLT) that combines data blocks in a chronological order and ensures that, by using cryptography [8], they cannot be tampered with or forged. The consensus mechanism is the core secret of blockchain network. In brief, the consensus mechanism is the mechanism by which the blockchain nodes achieve a whole-network consensus regarding blockchain information, which guarantees that the latest blocks can be accurately added to the blockchain, and that blockchain information stored in the node is uniform and not forked and can even withstand malicious attacks.

In a classical blockchain system, the core advantages are non-tampering, point-to-point transitivity, as well as distributed storage and privacy protection, while its most serious drawback is that the applied consensus mechanism wastes a great deal of computing resources and energy, making the system throughput low and the delay large [9]. Furthermore, the blockchain system cannot withstand a 51% attack. In a so-called 51% attack [10], that is, if more than 50% computational ability to mine hash values on the network is controlled by a group of miners, the attacker can prevent new transactions from receiving confirmation, and allow themselves to stop the payments of some or all users. They can also revoke transactions completed at a time when they have gained control of the network, which means they can perform a double-spend attack.

Fundamentally, the consensus mechanism of the classical blockchain system is based on a classical cryptography (mathematical cryptography) system which is based on an intractable problem of computational complexity. With computational power increasing, this kind of cryptography system can be easily breached, which is an inherent drawback of classical cryptography. However, quantum cryptography designed on the basis of the physical properties of quantum mechanics, whose security is guaranteed by the physical properties of the quantum information, is not based on the mathematical computational complexity problem. It is therefore not related to the attacker's computational power or the scale of their computational resources. No matter how powerful the attacker's computational power and computational resources are, it does not pose a threat to security of the system, which is often called the "unconditional security" of quantum cryptography. In recent years, various types of quantum signature schemes have been proposed, and various quantum signatures schemes [11–15], such as various quantum payment systems, mobile quantum payment systems [16–20] and so on, have also been studied. These provide new ideas for using quantum cryptography technology to study and design quantum blockchain systems.

In order to overcome these disadvantages of the consensus mechanism of the classical blockchain system and to achieve unconditional security, in our previous work [21], we proposed a quantum blockchain consensus mechanism based on the randomness and irreversibility of quantum measurement and quantum zero-knowledge proofs. However, this consensus mechanism is complicated and hard to realize.

In this paper, we propose a new quantum blockchain consensus mechanism based on quantum cryptography and the randomness of quantum teleportation and quantum measurement. This quantum blockchain consensus mechanism also has "unconditional security", which is analyzed in Section 4. Moreover, the consensus mechanism does not occupy a lot of computing resources, avoids the defect that the classical blockchain system cannot withstand 51% attacks, requires a low energy consumption, large throughput, small delay and is much easier to realize than our previous work [22].

The rest of paper is organized as follows. We introduce some fundamental theories in Section 2, including measurement basis, quantum measurement and quantum teleportation. In Section 3, we outline the blockchain consensus mechanism based on quantum teleportation, and some characteristics of the consensus mechanism are analyzed in Section 4. In Section 5, we conclude our work.

2. Fundamental Theory

2.1. Measurement Basis and Quantum Measurement

Since the quantum blockchain consensus mechanism proposed in this paper is based on quantum teleportation, in order to aid the reader's understanding, we introduce some fundamental theories of quantum mechanics in this section.

2.1.1. Measurement Bases B_Z and B_X

In quantum mechanics, a quantum measurement can be described by a set of measurement operators $\{M_m\}_{0\leq m\leq n}$, where $M_m = |m\rangle\langle m|$, $0 \leq m \leq n$ and $\sum_{m=0}^{n} M_m^{\dagger} M_m = I$. This means the quantum measurement can also be described by a set of bases $\{|m\rangle\}_{0\leq m\leq n}$. Two kinds of non-orthogonal single-qubit measurement bases are used in this paper—basis B_Z and basis B_X.

$B_Z = \{|0\rangle, |1\rangle\}$ is the first orthonormal basis, where $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Let

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{1}$$

One can see that $\{|+\rangle, |-\rangle\}$ forms another orthonormal basis, which is called B_X. It is easy to verify that these two bases B_Z and B_X are non-orthogonal, which satisfies

$$\langle B_Z | B_X \rangle = \frac{1}{\sqrt{2}}$$

From Equation (1), we have

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle), \quad |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \tag{2}$$

2.1.2. Quantum Measurement

In quantum mechanics, using a different measurement basis may lead to a different measurement result. For instance, supposing that a qubit is in the state $|0\rangle$ and we measure it with respect to basis B_Z, the measurement outcome must be state $|0\rangle$ since $|0\rangle$ is an eigenvector of $B_Z = \{|0\rangle, |1\rangle\}$. However, if we perform a measurement on it with respect to basis B_X, according to Equation (2) we will obtain state $|+\rangle$ with probability 50%, or state $|-\rangle$ with probability 50%, which is uncertain. In the same way, if a qubit is in the state $|+\rangle$ and we measure it in basis B_X, the measurement outcome must be in the state $|+\rangle$ since $|+\rangle$ is an eigenvector of B_X. However, if we measure it in basis B_Z, according to Equation (1) we will obtain state $|0\rangle$ with a probability of 50%, or state $|1\rangle$ with a probability of 50%, which is also uncertain. If we want to obtain a certain measurement result, we should choose the correct measurement basis so that the state of the qubit measured is one of the eigenvectors of the measurement basis. Otherwise, the measurement result is uncertain.

2.1.3. Bell Basis

For a two qubits system, the Bell basis is a frequently-used complete orthogonal basis denoted by $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$, where

$$|\Phi^+\rangle = \frac{1}{2}(|00\rangle + |11\rangle), \tag{3a}$$

$$|\Phi^-\rangle = \frac{1}{2}(|00\rangle - |11\rangle), \tag{3b}$$

$$|\Psi^+\rangle = \frac{1}{2}(|01\rangle + |10\rangle), \tag{3c}$$

$$|\Psi^-\rangle = \frac{1}{2}(|01\rangle - |10\rangle), \tag{3d}$$

These can be used as a complete orthogonal measurement basis for the Bell-basis joint measurement of a two qubits system. The quantum states denoted by Equation (3a,d) are known as the Bell states since they cannot be expressed as a tensor product of the single qubit basis $\{|0\rangle, |1\rangle\}$. They are entangled states and are named EPR (Einstein–Podolsky–Rosen) pairs. Bell states play important roles in quantum cryptography.

2.2. Quantum Teleportation

Quantum teleportation is an important application of quantum entanglement. The basic idea of "quantum teleportation" is as follows [21,23]: to transmit an unknown quantum state, its information can be separated into two parts—classical information and quantum information—which is transmitted to a remote receiver via a classical channel and a quantum channel, respectively. The receiver can recover the original quantum state, which is to be transmitted from the qubit in their possession according to these two pieces of information, namely, a long-distance transmission of a quantum state is realized. This transmission of a quantum state is not limited by time and space, and is not blocked by obstacles. The original qubit is still in the sender's possession, and its state is destroyed during the measurement with respect to the Bell basis of teleportation. Therefore, quantum teleportation does not violate the no-cloning theorem. Classical information needs to be transmitted in the process of quantum teleportation, so the speed of quantum teleportation is not faster than that of light.

Next, we simply describe the process of quantum teleportation. Assume that the sender is Alice, and the receiver is Bob. Alice's qubit which is to be transmitted is in the following state:

$$|\varphi\rangle_M = a|0\rangle_M + b|1\rangle_M = \begin{bmatrix} a \\ b \end{bmatrix}_M, \ |a|^2 + |b|^2 = 1 \tag{4}$$

She simultaneously prepares an EPR pair, which is composed of qubit A and qubit B:

$$|\Phi^+\rangle_{AB} = \frac{1}{2}\left(|00\rangle + |11\rangle\right)_{AB} \tag{5}$$

The entangled pair of qubits A and B is the quantum channel. Alice keeps qubit A in her possession and transmits qubit B to Bob. Now the mixed state of the 3 qubits is

$$\begin{aligned} |\Psi\rangle_{\mathrm{MAB}} &= |\varphi\rangle_{\mathrm{M}} \otimes |\Phi^+\rangle_{\mathrm{AB}} = (a|0\rangle + b|1\rangle)_{\mathrm{M}} \otimes \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{\mathrm{AB}} \\ &= \tfrac{1}{2}[|\psi^-\rangle_{\mathrm{MA}}(-b|0\rangle + a|1\rangle)_{\mathrm{B}} + |\psi^+\rangle_{\mathrm{MA}}(b|0\rangle + a|1\rangle)_{\mathrm{B}} + \\ &|\Phi^-\rangle_{\mathrm{MA}}(a|0\rangle - b|1\rangle)_{\mathrm{B}} + |\Phi^+\rangle_{\mathrm{MA}}(a|0\rangle + b|1\rangle)_{\mathrm{B}}] \\ &= \tfrac{1}{2}|\psi^-\rangle_{\mathrm{MA}}\begin{bmatrix} -b \\ a \end{bmatrix}_{\mathrm{B}} + \tfrac{1}{2}|\psi^+\rangle_{\mathrm{MA}}\begin{bmatrix} b \\ a \end{bmatrix}_{\mathrm{B}} + \tfrac{1}{2}|\Phi^-\rangle_{\mathrm{MA}}\begin{bmatrix} a \\ -b \end{bmatrix}_{\mathrm{B}} + \tfrac{1}{2}|\Phi^+\rangle_{\mathrm{MA}}\begin{bmatrix} a \\ b \end{bmatrix}_{\mathrm{B}} \end{aligned} \tag{6}$$

Alice measures qubits M and A in the Bell basis, and she sends the measurement result to Bob. According to Equation (6), Bob's qubit B will collapse into a corresponding state immediately after Alice's measurement. Then Bob can recover the state, which is the same as the original state of qubit M, from qubit B by performing the corresponding quantum operation.

For example, if Alice measures qubits M and A in the Bell basis and the measurement result is $|\psi^-\rangle_{MA}$, according to Equation (6), Bob's qubit B will collapse into state $-b|0\rangle + a|1\rangle$. Then Bob performs the Pauli Y operation ($Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$) on it and can recover the original state $a|0\rangle + b|1\rangle$ of M that is to be transmitted. Similarly, when the results of measuring qubits M and A are $|\Psi^+\rangle_{MA}$, $|\Phi^+\rangle_{MA}$, $|\Phi^-\rangle_{MA}$, respectively, in order to recover the original state, Bob should perform the quantum NOT gate $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, quantum Z gate $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and identity operator $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ on qubit B, respectively.

3. Blockchain Consensus Mechanism Based on Quantum Teleportation

There are two main roles in a quantum blockchain system: users and miners. Users use quantum currency for transactions, and miners compete for mining, compete for bookkeeping rights, and generate blockchain.

We take proof of work as an example to briefly introduce the basic steps of classical blockchain consensus mechanism:

(1) Nodes, namely miners, monitor the data records of the whole network, and the data records that pass the basic legitimacy verification are temporarily stored.

(2) Nodes use their own computing power to try different nonces, perform the specified hash calculation, and repeat the process until a reasonable nonce is found. This process is also known as "mining".

(3) After finding a reasonable nonce, nodes generate block information (Block header + Block body).

(4) Nodes broadcast the newly generated block to the outside. After other nodes pass the verification, the block is connected to the blockchain, and the height of the main chain is increased by one. Then all nodes switch to the new block and continue to the next round of mining.

The major disadvantages of the classical consensus mechanism of blockchain are as follows. On the one hand, in the process of "mining", nodes consume their computing power to try different nonces, which wastes computing resources and energy, consumes a lot of computing resources, and causes the system to have a low throughput and large time delay. On the other hand, if a group of miners controls more than 50% of the computing power to mine the hash values of the network, the attackers can prevent new transactions from being confirmed and can stop payments between some or all users, which is known as a "51% attack".

The blockchain consensus mechanism based on quantum teleportation, which will not consume any computing power and only performs some quantum operators, is entirely different from the above classical blockchain consensus mechanism. The quantum consensus mechanism of the blockchain system is briefly described as follows. The quantum consensus mechanism can be referred to as a "lottery betting" quantum consensus mechanism. Firstly, a transaction user generates nonce S through quantum operations, which is similar to the "winning number" in lottery betting, and the nonce is confidential. Then a miner selects a nonce S', which is similar to the "betting number" in lottery betting (if the nonce selected by the miner has been selected by other miners, the system will show that the nonce has been selected and allow the miner to choose another nonce). Finally, through quantum teleportation, if $S' = S$, the miner obtains the accounting right and generates block information. The detailed steps of the quantum blockchain consensus mechanism are as follows.

3.1. Protocol Initialization

Step 1: **Preparation of quantum channel**. Miner Alice prepares N' groups of EPR pairs which are shown in Equation (5). She keeps qubit A and sends qubit B to transaction user Bob.

Step 2: **Security detection of quantum channel**. The EPR pair as shown in Equation (5) can be represented in bases B_Z and B_X, respectively, as

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle) = \frac{1}{\sqrt{2}}(|+_A +_B\rangle + |-_A -_B\rangle) \tag{7}$$

In order to prevent an attack by intermediators, interception/retransmission attack or entanglement/measurement attack, the security of the quantum channel can be detected in advance. Alice randomly chooses $(N' - N)$ qubits from a sequence of qubits A in her possession, randomly measures these qubits for the basis B_Z or B_X and informs Bob of the indexes of these qubits in the sequence, the corresponding measurement basis and the corresponding measurement results through the classical channel. According to Equation (7), without an attack, when Alice's measurement result is state $|+\rangle$, the state of Bob's qubit must collapse into the $|+\rangle$ state; when Alice's measurement result is state $|-\rangle$, the state of Bob's qubit must collapse into the $|-\rangle$ state; when Alice's measurement result is state $|0\rangle$, the state of Bob's qubit must collapse into the $|0\rangle$ state, and so on. After receiving Alice's announcement, Bob successively measures the corresponding indexed qubit B for a correct basis. Alice and Bob openly compare the measurement results. If the measurement results are the same, it indicates that the channel is secure. The remaining N groups of EPR pairs are used as quantum channels. Of course, the quantum channels can be identified by other methods [24].

Step 3: **Quantum key distribution**. Alice and Bob share the secret key ($2N$-bit). The key distribution can be realized by BB84, BBM92 or other mature quantum key distribution protocols [25–27].

3.2. Generating Nonce S

In real life, winning numbers of a lottery ticket are randomly generated by a "lottery", but the nonce S of transaction users is randomly generated by quantum measurement results. Transaction users prepare N qubits in the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$$

and measure a sequence of N qubits under basis B_Z. The measurement results are encoded as a binary number according to the following equation. The nonce S needs to be highly confidential before determining which miner is successful in mining.

$$|0\rangle \to 0,\ |1\rangle \to 1$$

3.3. Process of Mining Based on Consensus Mechanism

Mining is the process of finding nonce S and verifying $S' = S$ by quantum methods. In the process, miners cannot obtain any useful information from nonce S. The miner chooses a nonce S' as a secret number (each miner only has a chance to choose), and then indirectly compares S' with the nonce S of a quantum blockchain system user via quantum teleportation. If the verification is passed, the miner finds a legal block. The detailed process is as follows.

Step 1: Since Alice and Bob both have secret numbers S' and S, Alice can prepare an information qubit sequence M according to her secret number $S' = \{S'_i, i = 1, 2, \cdots, N\}$ by the following rule. This rule is overt.

Alice prepares an information qubit sequence M according to the rule

$$\begin{cases} if\ S_i = 0, & take\ |\varphi\rangle_M = |0\rangle \\ if\ S_i = 1, & take\ |\varphi\rangle_M = |+\rangle \end{cases} \tag{8}$$

Step 2: Alice performs joint measurements on the qubit sequence M and A with respect to the Bell basis, and the measurement result is one of the four Bell states shown in Equation (3a,d). These four measurement results can be encoded into two classical bits of information:

$$|\Psi^-\rangle \to 00,\ |\Psi^+\rangle \to 01,\ |\Phi^-\rangle \to 10,\ |\Phi^+\rangle \to 11 \tag{9}$$

Alice denotes the $2N$ bits of information of the measurement on the qubit sequence M and A as $P = \{P_i\}$, encrypts them with the key K_{AB} shared with Bob and sends them to him.

Step 3: Bob decrypts the encrypted information of Alice above with the shared key K_{AB} to obtain the classical information $P = \{P_i\}$, and performs the corresponding quantum gate on the corresponding qubit of the qubit sequence B according to $\{P_i\}$. The correspondence rule of $\{P_i\}$ and the corresponding quantum gate is

$$00 \to Y,\ 01 \to X,\ 10 \to Z,\ 11 \to I \tag{10}$$

Step 4: After performing the corresponding quantum gate, Bob measures each qubit of the sequence B with respect to the corresponding basis according to his secret number $S = \{S_i\}$ by the following rule

The rule by which Bob selects the basis for measuring a qubit of the sequence B is

$$\begin{cases} if\ S_i = 0, & in\ basis\ B_Z \\ if\ S_i = 1, & in\ basis\ B_X \end{cases} \tag{11}$$

If $S' = S$, the measurement result must be one of the quantum states $\{|0\rangle, |+\rangle\}$, since according to Alice's nonce S', she has transferred the state $\{|0\rangle, |+\rangle\}$ of the information qubits sequence M, which is shown in Equation (8) to the qubits sequence B in Bob's possession by quantum teleportation. If Bob takes the correct measurement basis according to Equation (11), he must obtain the eigenvector $|0\rangle$ (or $|+\rangle$) of the corresponding basis, which means that the result of the measurement is determined. If the measurement result is in the other state, which means the nonce S' selected by Alice is not equal to nonce S, Alice is abandoned. Otherwise, the verification passes, and Alice is selected, which means she has found the legal block of user Bob.

If a miner who has found a legal block broadcasts the legal block to other miners through a P2P network and the block is recognized by other miners, the miner will have the bookkeeping right to the block and will receive the resulting income (quantum currency).

4. Characteristic Analysis

In this section, we analyze some characteristics of our proposed quantum blockchain consensus mechanism, including unconditional security, the zero-knowledge of secret number S, the ability to withstand a 51% attack, low energy consumption, small delay and large throughput.

4.1. Unconditional Security

This scheme applies the randomness of the collapse of quantum measurements and quantum teleportation technology, rather than a mathematically intractable problem based on cryptography such as in the classical blockchain protocol. Therefore, the security of our scheme is based on quantum physical characteristics and has nothing to do with the attacker's computing power and computing resources; that is to say, the scheme has unconditional security.

4.2. Zero-Knowledge of Secret Number S

In this scheme, the confidentiality of the nonce (winning number) S generated by user Bob is zero-knowledge for miner Alice. Alice cannot infer any information about user Bob's nonce S from the verification process. Since the information between Alice and Bob is merely that they share the secret key K_{AB}, and there is no information sent by Bob to Alice, Alice cannot obtain any information about Bob's nonce S from the verification process.

4.3. Advantages of the Scheme

4.3.1. Withstanding a 51% Attack

Since the design of our scheme adopts quantum methods, such as quantum measurement and quantum teleportation, rather than a hash function like the classical blockchain protocol, it avoids the defect that the classical blockchain protocol cannot withstand attacks exceeding 51% of the computing power of the whole network.

4.3.2. Low Energy Consumption, Small Delay and Large Throughput

In the classic blockchain system, nodes need to perform complex mathematical operations in mining competition which absorbs many computing resources. Therefore, it will consume much energy and computing time, resulting in a high energy consumption, low throughput and large delay. Taking the Bitcoin system as an example, its throughput can theoretically only process 14 transactions per second, each transaction takes at least 10 min to be confirmed, and large transactions even take more than an hour to be finally confirmed. This is far from the tens of thousands of transactions that banks and other centralized systems often need to process per second.

Our scheme adopts the physical characteristics of quantum measurement and quantum teleportation technology to determine the success of miners' mining, which avoids absorbing a large amount of computing resources in mining competition, so the energy consumption is very low. At the same time, it avoids a large number of mathematically complex calculations required in mining competition; thus, it saves computing resources. The time required for quantum teleportation is very short and mainly includes the time taken for classical information transmission and performing quantum gates, and the transmission of the quantum state is instantaneously completed. Thus, theoretically, the throughput is large, and the delay is small.

5. Conclusions

In this paper, using the randomness of quantum measurement and quantum teleportation technology, we propose a new consensus mechanism for a quantum blockchain system which is different from that of a classical blockchain system. Because the scheme is based on the physical characteristics of quantum mechanics, it has the unconditional security of quantum cryptography, the theory of which is analyzed in Section 3. In addition, compared with the classical blockchain consensus mechanism, it also has the following obvious advantages: the consensus mechanism uses the randomness of quantum measurement to generate nonces and quantum teleportation technology to determine which miner is successful. Therefore, it does not use a lot of computing resources, avoids the defect that the classical blockchain system cannot withstand 51% attacks, and realizes a low energy consumption, large throughput and small delay. Furthermore, compared with the previous quantum blockchain consensus mechanism, it is much easier to implement.

Author Contributions: All authors conceived the work, analyzed the results and wrote the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partially supported by the National Key Research and Development Program of China (No. 2018YFB1801900, No. 2019YFE0123600), National Natural Science Foundation of China (No. 62171202, No. 62075088).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Christidis, K.; Devetsikiotis, M. Blockchain and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
2. Yang, Z.; Zheng, K.; Yang, K.; Leung, V.C. A blockchain-based reputation system for data credibility assessment in vehicular networks. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017.
3. Herbaut, N.; Negru, M. A model for collaborative blockchain-based video delivery relying on advanced network services chain. *IEEE Commun. Mag.* **2017**, *55*, 70–76. [CrossRef]
4. Lei, A.; Cruickshank, H.; Cao, Y.; Asuquo, P.; Ogah, C.P.P.A.; Sun, Z. Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems. *IEEE Int. Things J.* **2017**, *4*, 1832–1842. [CrossRef]
5. Cai, C.; Yuan, X.; Wang, C. Hardening Distributed and Encrypted Keyword Search via Blockchain. In Proceedings of the 2017 IEEE Symposium on Privacy-Aware Computing (PAC), Washington, DC, USA, 1–4 August 2017.
6. Cai, C.; Yuan, X.; Wang, C. Towards trustworthy and private keyword search in encrypted decentralized storage. In Proceedings of the 2017 IEEE International Conference on Communications, Paris, France, 21–25 May 2017.
7. Wang, A.; Fan, J.; Guo, Y. Application of blockchain in energy interne. *Electr. Power Inf. Commun. Technol.* **2016**, *14*, 1–6.
8. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* **2008**, *4*, 21260.
9. Zeng, Z.; Li, Y.; Cao, Y.; Zhao, Y.; Zhong, J.; Sidorov, D.; Zeng, X. Blockchain technology for information security of the energy internet: Fundamentals, features, strategy and application. *Energies* **2020**, *13*, 881. [CrossRef]
10. Sayeed, S.; Marco-Gisbert, H. Assessing blockchain consensus and security mechanisms against the 51% attack. *Appl. Sci.* **2019**, *9*, 1788. [CrossRef]
11. Wen, X.; Niu, X.; Ji, L.; Tian, Y. A weak blind signature scheme based on quantum cryptography. *Opt. Commun.* **2009**, *282*, 666–669. [CrossRef]
12. Jiang, D.; Xu, Y.; Xu, G. Arbitrary quantum signature based on local indistinguishability of orthogonal product states. *Int. J. Theor. Phys.* **2019**, *58*, 1036–1045. [CrossRef]
13. Wen, X.; Tian, Y.; Ji, L.; Niu, X. A group signature scheme based on quantum teleportation. *Phys. Scr.* **2010**, *81*, 055001. [CrossRef]
14. Qin, H.; Tang, W.; Tso, R. Efficient quantum multi-proxy signature. *Quantum Inf. Processing* **2019**, *18*, 53. [CrossRef]
15. Shi, W.M.; Wang, Y.M.; Zhou, Y.H.; Yang, Y.G. Cryptanalysis on quantum digital signature based on asymmetric quantum cryptography. *Optik* **2018**, *154*, 258–260. [CrossRef]

16. Zhang, J.; Hu, M.; Jia, Z.; Wang, L. A novel E-payment protocol implented by blockchain and quantum signature. *Int. J. Theor. Phys.* **2019**, *58*, 1315–1325. [CrossRef]
17. Wen, X. An E-payment system based on quantum group signature. *Phys. Scr.* **2010**, *82*, 065403.
18. Wen, X.; Chen, Y.; Fang, J. An inter-bank E-payment protocol based on quantum proxy blind signature. *Quantum Inf. Proc.* **2013**, *12*, 549–558. [CrossRef]
19. Wen, X.; Chen, Y.; Zhang, W.; Jiang, Z.L.; Fang, J. A Mobile Quantum Payment Protocol Based on the Entanglement Coherence of Four-particle GHZ State. *J. Internet Technol.* **2019**, *20*, 1861–1868.
20. Niu, X.; Zhang, J.; Xie, S.; Chen, B. A practical e-payment protocol based on quantum multi-proxy blind signature. *Commun. Theor. Phys.* **2018**, *70*, 529. [CrossRef]
21. Wen, X.; Chen, Y. *Quantum Signature and Its Application*; Aviation Industry Press: Beijing, China, 2012; pp. 35–38.
22. Wen, X.; Chen, Y.; Fan, X.; Zhang, W.; Yi, Z.; Fang, J. Blockchain consensus mechanism based on quantum zero-knowledge proof. *Opt. Laser Technol.* **2022**, *147*, 107693. [CrossRef]
23. Fan, X.; Wen, X. Improvement of data link layer algorithm based on quantum teleportation. *Chin. J. Quantum Electron.* **2015**, *32*, 466.
24. Dong, Y.; Peng, J. Quantum channel authentication scheme via weak cross-Kerr nonlinearity. *J. Quantum Optic.* **2015**, *21*, 334–338.
25. Zhou, Y.; Li, X.; Zhou, X. Study on BB84-decoy-state quantum key distribution with a heralded single photon source. *Chin. J. Quantum Electron.* **2010**, *27*, 565–572.
26. Wu, Z.; Chen, G.; Yang, B. Improve the performance of BBM92 quantum key distribution system. *Chin. J. Quantum Electron.* **2009**, *26*, 560–564.
27. Mao, Q.; Zhao, S.; Wang, L.; Qian, C.; Chen, H. Measurement-device-independent quantum key distribution based on wavelength division multiplexing technology. *Chin. J. Quantum Electron.* **2017**, *34*, 46–53.