Efficient Quantum Blockchain With a Consensus Mechanism QDPoS

Qin Li, *Member, IEEE*, Jiajie Wu, Junyu Quan, Jinjing Shi, *Member, IEEE*, and Shichao Zhang, *Senior Member, IEEE*

***Abstract*— Quantum blockchain is expected to offer an alternative to classical blockchain to resist malicious attacks laughed by future quantum computers. Although a few quantum blockchain schemes have been constructed, their efficiency is low and unable to meet application requirements due to the fact that they lack of a suitable consensus mechanism. To tackle this issue, a consensus mechanism called quantum delegated proof of stake (QDPoS) is constructed by using quantum voting to provide fast decentralization for the quantum blockchain scheme at first. Then an efficient scheme is proposed for quantum blockchain based on QDPoS, where the classical information is initialized as a part of each single quantum state and these quantum states are entangled to form the chain. Compared with previous methods, the designed quantum blockchain scheme is more complete and carried out with higher efficiency, which greatly contributes to better adapting to the challenges of the quantum era.**

***Index Terms*— Quantum blockchain, consensus mechanism, QDPoS, quantum voting, quantum entanglement.**

I. Introduction

BLOCKCHAIN is a tamper-evident, open, transparent and distributed ledger maintained by all nodes together, which was first proposed by Nakamoto in 2008 [1]. It is an integration of multiple technologies, including decentralization techniques, cryptography and consensus mechanisms. As it enables a peer-to-peer transaction system that eliminates third trusted parties, blockchain has been widely used in various fields, such as financial technology [2], [3], supply chain management [4], economics [5], outsourcing services [6], and personal data management [7]. In a blockchain scheme, every block is the vehicle for blockchain transactions and each transaction is verified by the use of digital signature. Up to now, some consensus algorithms, such as proof of work (PoW) [1], proof of stake (PoS) [8], delegated proof of Stake (DPoS) [9], and practical byzantine algorithm (PBFT) [10], have been successfully developed for blocks containing information on transactions that are decided to be generated and accepted by everyone. Each block is identified by a hash value which is generated by applying a suitable hash function to the data related to current transaction and the hash value of the previous block. By connecting the hashes, blocks form chains with each other. As well known, the security of blockchain mainly relies on the used consensus mechanism [8], [9], [10], hash function [11], [12], and digital signature [13], [14].

Recently, the development of quantum computing has threatened the security of blockchain. The main problem of classical blockchain lies in that it is possible to crack hash functions and classical digital signatures based on asymmetric cryptography if quantum computers are available. For example, Shor's quantum algorithm can factorize large integers and solve discrete logarithms in polynomial time [15]. This means, some digital signature algorithms based on such difficult problems [16] are easily attacked by quantum computers. In addition, consensus mechanisms in blockchain such as PoW and PoS rely on hashrate to compete for bookkeeping rights. Although Grover's quantum search algorithm only provides quadratic speedup for unordered database search [17], users with quantum computers to utilize it still have the advantage of calculating hash values compared with ordinary users and making the 51% attack possible [18] by controlling more than half of the total hashing power of the network. Therefore, how to ensure the security of blockchain is a significant issue in the quantum era.

Quantum cryptography based on the principles of quantum mechanics can be used to protect information and resist some quantum attacks. Since the first quantum key distribution (QKD) protocol was proposed in 1984 [19], various quantum cryptographic protocols have emerged one after another, such as quantum homomorphic encryption protocols [20], [21], quantum voting methods [22], [23], quantum image encryption [24], [25], and quantum digital signature [26], [27], [28]. How to use quantum cryptographic technologies to secure blockchains and construct quantum blockchains is getting more and more attention. In 2018, Ikeda and Kazuki built a peer-to-peer quantum cash system using quantum digital signature [29]. In the same year, Kiktenko *et al.* proposed a quantum-secured blockchain mainly by replacing digital signature in the classical blockchain with QKD and generating blocks in a decentralized fashion [30]. In 2019, Rajan and

Manuscript received 12 February 2022; revised 21 June 2022 and 28 July 2022; accepted 19 August 2022. Date of publication 31 August 2022; date of current version 20 September 2022. This work was supported in part by the Key Project of Hunan Province Education Department under Grant 20A471; in part by the Natural Science Foundation of Hunan Province under Grant 2018JJ2403 and Grant 2020JJ4750; and in part by the National Natural Science Foundation of China under Grant 62271436, Grant 61972418, Grant 62272483, and Grant 61836016. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Hossein Pishro-Nik. *(Corresponding authors: Jinjing Shi; Shichao Zhang.)*

Qin Li, Jiajie Wu, and Junyu Quan are with the School of Computer Science, Xiangtan University, Xiangtan 411105, China (e-mail: liqin@xtu.edu.cn; wujiajie07@qq.com; quanli91@qq.com).

Jinjing Shi and Shichao Zhang are with the School of Computer Science and Engineering, Central South University, Changsha 410083, China (e-mail: shijinjing@csu.edu.cn; zhangsc@mailbox.gxnu.edu.cn).

Digital Object Identifier 10.1109/TIFS.2022.3203316

1556-6021 © 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: University College Dublin. Downloaded on January 14,2025 at 17:12:14 UTC from IEEE Xplore. Restrictions apply.

Visser proposed a quantum blockchain scheme based on temporal entanglement [31], where GHZ states are used to encode the quantum blockchain and each quantum block can only represent two bits of classical information. In 2020, Banerjee *et al.* proposed a quantum blockchain protocol that uses weighted hypergraph states to record the information of classical blocks [32]. In addition, several other methods combining blockchain and quantum technologies also have been proposed [33], [34], [35], [36], [37], [38]. However, most of the presented quantum blockchains do not include effective verification methods and specific consensus algorithms, which may result in the information related to transactions not being verified and inefficiency of implementation. Quantum blockchain may have better performance if it needs less quantum resources and can process various transactions quickly.

Due to the computational advantage brought by quantum computers, it is obvious that consensus mechanisms that relies on hashrate such as PoW and PoS are not suitable for quantum blockchain. Instead, DPoS is based on voting and independent of the computing power of nodes, which is more in line with quantum blockchain. In addition, digital signature has been well integrated with classical blockchain. Similarly, the use of quantum digital signature can also be applied to quantum blockchain to effectively guarantee the authenticity of transactions. By constructing the first QDPoS consensus mechanism and integrating existing quantum digital signature methods, in this paper we propose an efficient quantum blockchain scheme where single qubits are used to generate quantum blocks and they are chained by entanglement. The security and the effectiveness of the proposed quantum blockchain scheme also can be ensured.

The main contributions of this paper are summarized as follows.

- A new consensus mechanism QDPoS based on quantum voting is proposed for normal nodes to reach an agreement and representative nodes to generate corresponding blocks fast. Furthermore, even if quantum computers are realized in the future, they will not affect the fairness of QDPoS.
- An efficient quantum blockchain scheme is proposed by designing quantum blocks with single qubits, linking quantum blocks in the weighted graph states or the weighted hypergraph states, and combining quantum digital signature and the designed consensus mechanism QDPoS.

The rest of the paper is organized as follows. Section II briefly reviews some work related to classical and quantum blockchain. In section III, a consensus algorithm QDPoS is constructed based on quantum voting. Section IV presents a new quantum blockchain scheme that combines various quantum technologies. Section V analyzes the security of the proposed scheme and makes comparisons with typical quantum blockchain schemes presented previously. Section VI gives a simple example of the proposed quantum blockchain scheme. The last section makes a conclusion of this paper.

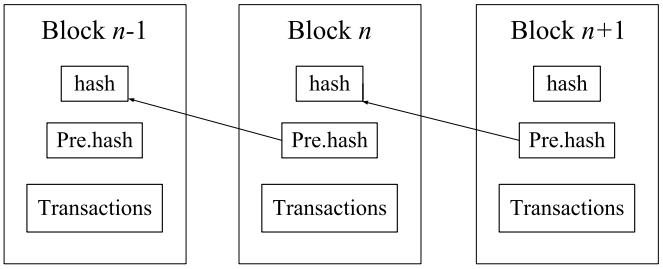

Fig. 1. Structure of the blockchain.

II. Related Work

In this section, we mainly introduce preliminaries and related work about classical blockchain and quantum blockchain.

A. Classical Blockchain and Challenges

1) Construction of Classical Blockchain: Classical blockchain can be considered as a distributed database with a data structure of contiguous blocks that are jointly maintained by all nodes through the hash function and the consensus mechanism [1], [39]. A transaction is a basic record of the classical blockchain. Once a transaction is generated, it usually needs to be digitally signed by the initiator and broadcasted in the blockchain network. A block consists of valid transactions occurring over a period of time, the hash value of the previous block, and the hash value of the current block. All the blocks form a chain as shown in Fig. 1. The generation of blocks is determined by the consensus mechanism, which aims to obtain the right for bookkeeping. The nodes for producing blocks can be selected by consensus algorithms such as PoW, PoS, and DPoS. Unlike PoW and PoS competing for block mining through hashrate, DPoS mainly elects representative nodes by voting to take turns bookkeeping the blocks. Thus DPoS does not require much resource consumption and it may be more in line with the blockchain in the quantum era. In order to create a new block, the selected node needs to check the validity of the transactions that occur during the specified time, discard invalid transactions, and generate a new block with valid transactions. After the new generated block is broadcasted throughout the whole blockchain network, each node verifies the validity of the block and adds it to the local copy of the blockchain.

2) Quantum Threats to Classical Blockchain: With the advent of quantum computers, the security of classical blockchain is threatened [34], [35]. In some classical blockchain schemes, the used digital signature algorithms are based on some difficult problems such as solving discrete logarithms or factorizing big integers. However, Shor's quantum algorithms can be employed to solve them in polynomial time [15] and thus make the corresponding classical digital signature schemes insecure. In addition, Grover's quantum search algorithm [17] can provide square-root acceleration for computing the inverse of hash functions, which means that the computational power of nodes with quantum computers is

Authorized licensed use limited to: University College Dublin. Downloaded on January 14,2025 at 17:12:14 UTC from IEEE Xplore. Restrictions apply.

greatly increased. In some blockchain schemes where PoW or PoS consensus methods were employed, block mining would be monopolized by nodes who own quantum computers and it may make the 51% attack possible [18]. In addition, if the voting methods used by DPoS are based on certain classical cryptographic algorithms threatened by quantum computers, DPoS may also suffer quantum attacks.

B. Quantum Blockchain

1) Basic Knowledge of Quantum Computation: Quantum computation is a disruptive and emerging computing paradigm based on the principles of quantum mechanics. The parallel computing capability of quantum computation provides a great computational advantage based on the feature of quantum superposition and can efficiently solve some complicated problems that cannot be solved in polynomial time with classical computation. Quantum computation uses a qubit as the unit of information. For example, any state of a qubit $|\varphi\rangle$ in $\mathbb{C}^2$ can be expressed as

$$|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{1}$$

where α, β are the probability magnitudes and $|\alpha^2|+|\beta^2| = 1$. For example, the following superposition state

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{2}$$

is usually used in various application. In contrast, the value of a classical bit can only be 0 or 1. For the state of multiple qubits, there are two forms, namely direct product states and entangled states. The property of entangled states is that they cannot be described as the tensor product of states of individual qubits.

In addition, the evolution of quantum states can be described by corresponding unitary operations and quantum gates are used to build quantum circuits. For instance, I, X, Y, Z, H, S, and T are typical single-qubit gates and the controlled-X (CNOT) and the controlled-Z (CZ) gates are two-qubit gates often used. Besides, multi-qubit gates such as the k-qubit controlled phase gate $\mathrm{C}^k\mathrm{Z}$ will be used in this paper, where k can be any positive integer.

2) Quantum Hypergraph States and Graph States: The quantum hypergraph states are a set of highly entangled multiparty quantum states that are constructed on a mathematical hypergraph [40]. The qubits are positioned on the vertices of the hypergraphs and the hyperedges show connections among some qubits. An inseparable many-body quantum state consisting of seven vertices and three hyperedges is shown in Fig. 2. When each hyperedges in a N-qubit hypergraph state carries weight, the state is called a weighted hypergraph state [41], [42] and can be described as

$$|\phi\rangle = \frac{1}{\sqrt{2^N}} \sum_{j\in(0,1)^N} e^{i\pi f(j)}\,|j\rangle\,, \tag{3}$$

where $|j\rangle$ represents the computation basis state and $f(j)$ represents the corresponding weight value.

Similar to quantum hypergraph states, the quantum graph states are multi-particle entangled states that correspond to

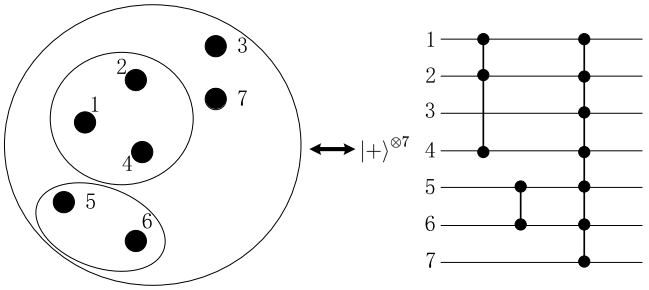

Fig. 2. A quantum hypergraph state with seven vertices, where a 2-hyperedge connects vertices 5 and 6, a 3-hyperedge connects vertices 1, 2, and 4, and a 7-hyperedge connects all seven vertices.

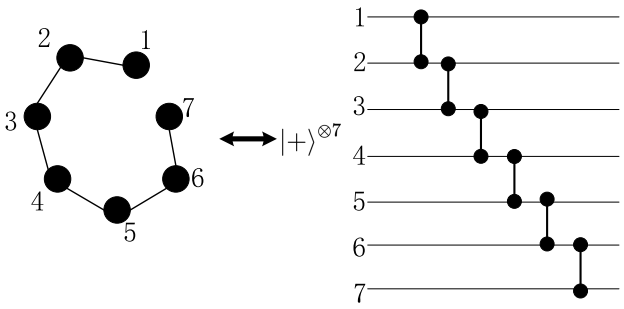

Fig. 3. A quantum graph state with seven vertices.

mathematical graphs [43]. Unlike the hyperedges in the quantum hypergraph state, which can contain more than three vertices, the edges in the quantum graph state contain only two vertices. A quantum graph state with seven vertices is shown in Fig. 3.

3) Quantum Blockchain Using Weighted Hypergraph States: In Ref. [32], Banerjee *et al.* proposes a quantum blockchain scheme by using weighted hypergraph states. The classical information contained in blocks are in the form of phases of single qubits, also called weights. These single qubits are the vertices of the corresponding hypergraph states and they are connected through entanglement. The processes of the protocol are as follows.

A quantum block is constructed by converting classical information p into a phase loaded onto the quantum state $\frac{|0\rangle+e^{i\theta_p}|1\rangle}{\sqrt{2}}$. Then the phase angles of the quantum blocks are set to be equiproportional

$$\theta_{p_i} = \frac{1}{q^{i-1}}\theta_{p_1}, \tag{4}$$

where θ_{p_1} and θ_{p_i} are the phase angles of the first quantum block and the i-th quantum block respectively, q is a positive integer bigger than 1, and $\frac{1}{q}$ is the constant ratio of the geometric progression series. This means that after the first quantum block is determined, the subsequent quantum blocks can all be determined by the equal proportional relation between phase angles to reach consensus. Finally, all the quantum blocks are entangled into a weighted hypergraph state to form a quantum blockchain. For example, the quantum blockchain with three quantum blocks is shown in Fig. 4.

4) Two Important Entangled States in a Quantum Voting Protocol Suitable for Consensus Mechanism: Voting has a

Authorized licensed use limited to: University College Dublin. Downloaded on January 14,2025 at 17:12:14 UTC from IEEE Xplore. Restrictions apply.

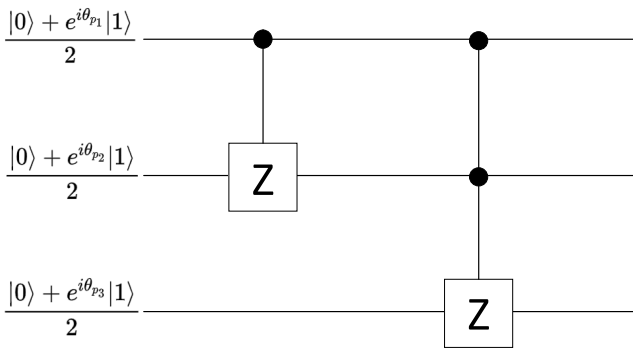

Fig. 4. Circuit diagram of a weighted hypergraph state with three quantum blocks.

wide range of applications in some consensus mechanisms designed for blockchain schemes. Most of classical voting schemes are based on public-key cryptographic algorithms, which may be cracked by quantum algorithms. But quantum voting schemes based on the principles of quantum mechanics can resist attacks initiated by quantum computers. Recently, Wang *et al.* proposed a quantum voting protocol by using two special quantum entangled states [23], which is fair, private, self-tallying, verifiable, and non-reusable. By using the computational basis $\{|j\rangle_C, j = 0, 1, \ldots, m-1\}$, the first m-level and n-particle quantum entangled state $|\delta_n\rangle$ is described as

$$|\delta_n\rangle \equiv \frac{1}{m^{\frac{n-1}{2}}} \sum_{\sum_{k=0}^{n-1} j_k \bmod m = 0} |j_0\rangle_C |j_1\rangle_C \cdots |j_{n-1}\rangle_C . \quad (5)$$

It can be rewritten as

$$|\delta_n\rangle = \frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |j'\rangle_{\mathcal{F}} |j'\rangle_{\mathcal{F}} \cdots |j'\rangle_{\mathcal{F}}, \quad (6)$$

where

$$|j'\rangle_{\mathcal{F}} = \mathcal{F}|j\rangle_C = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} e^{\frac{2\pi i j k}{m}} |k\rangle_C, \quad (7)$$

and $\{|j'\rangle_{\mathcal{F}}, j = 0, 1, \ldots, m-1\}$ is the Fourier basis. Note that if $|\delta_n\rangle$ is measured in the computational basis, the sum of the measurements of all particles modulo m is equal to 0, and if it is measured in the Fourier basis, the measurement result is the same for all particles. The other n-level and n-particle quantum entangled state being used is $|\eta_n\rangle$, described as

$$|\eta_n\rangle \equiv \frac{1}{\sqrt{n!}} \sum_{S \in P_n^n} (-1)^{\tau(S)} |s_0\rangle |s_1\rangle \cdots |s_{n-1}\rangle , \quad (8)$$

where P_n^n is all permutations of $\{0, 1, \ldots, n-1\}$, $S = s_0 s_1 \cdots s_{n-1} \in P_n^n$, and $\tau(S)$ is the inverse order of S. $|\eta_n\rangle$ has the property that the measurement results are different for each particle not matter when it is measured in the measurement basis or in the Fourier basis.

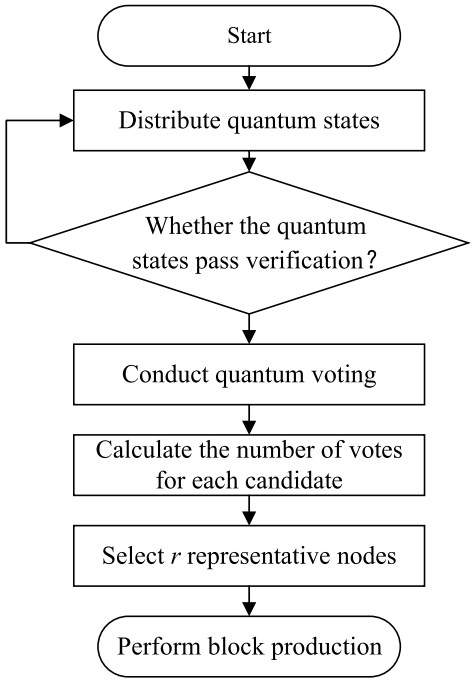

Fig. 5. Block producton by using QDPoS.

III. Quantum Delegated Proof of Stake

Delegated proof of stake (DPoS) is a voting-based consensus mechanism that is one of the key factors in ensuring the decentralization of blockchain as well as maintaining consistency. It allows nodes to vote for several representative nodes that exercise their power on their behalf to increase the throughput of the blockchain and reduce latency. Unlike PoW and PoS consensus methods, which consumes a lot of computing power, DPoS reaches consensus through democratic elections, which is more in line with the blockchain. However, the security of most classical voting protocols is based on the assumption of the computational complexity of certain mathematical problems, such as large integer decomposition and discrete logarithm solving. Some quantum algorithms [15], [17] can solve such problems to make these voting protocols no longer be secure, and thus the consensus mechanism DPoS based on them is likely vulnerable to quantum attacks. In this section, a quantum consensus mechanism QDPoS is constructed by using an improved quantum voting scheme. It not only can keep similar advantages of classical DPoS, but also is able to resist quantum attacks benefiting from the original quantum voting protocol in Ref. [23].

Similar to the construction of classical DPoS, QDPoS elects a certain number of representative nodes through quantum voting and the representative nodes generate new blocks as shown in Fig. 5. It includes the following four steps.

Step 1: Election of representative nodes. Suppose the number of representative nodes $R_1, R_2, \cdots, R_r$ to be elected is r and each node votes through an improved quantum voting scheme.

The original quantum voting protocol proposed in Ref. [23] can be used for electing representative nodes, but it is

Authorized licensed use limited to: University College Dublin. Downloaded on January 14,2025 at 17:12:14 UTC from IEEE Xplore. Restrictions apply.

inefficient during the security testing phase and each node can only cast one positive vote. Thus we improve it to be more adaptable to quantum blockchain. In the improved protocol, each node can vote positively, negatively, and abstain from voting and the distribution of quantum states is done by the distribution center CA. To make the voting be diverse, we extend the m-level and n-particle quantum state $|\delta_n\rangle$ given in Eq. 5 to the $2m+1$-level and n-particle quantum state

$$|\zeta_n\rangle \equiv \frac{1}{l^{\frac{n-1}{2}}} \sum_{\sum_{k=0}^{n-1} j_k \bmod l = 0} |j_0\rangle_C |j_1\rangle_C \cdots |j_{n-1}\rangle_C , \quad (9)$$

where $l = 2m+1$. Ballot boxes are distributed to voters by using states $|\zeta_n\rangle$ and voters have a ballot range of $[0, \cdots, 2m]$. Assume that m candidates are indexed as $0, 1, \cdots, m-1$. Then the ballots belonging to $[0, \cdots, m-1]$ represent the positive votes for candidates $0, 1, \cdots, m-1$, the ballots belonging to $[m, \cdots, 2m-1]$ represent the negative votes, and the ballot $2m$ represents the abstention, respectively. Moreover, the distribution of one quantum state $|\eta_n\rangle$ as Eq. 8 and n quantum states $|\zeta_n\rangle$ as Eq. 9 is done through representative nodes, which only need to insert trap qubits in the sequence of quantum states assigned to voters to ensure secure distribution. But in Ref. [23], the generation and distribution of quantum states is performed by a random voter, therefore $n+n\varepsilon_0$ copies of the quantum state $|\delta_n\rangle$ and $1+n\varepsilon_1$ copies of the quantum state $|\eta_n\rangle$ are needed, where $\varepsilon_0, \varepsilon_1$ are security parameters. It means $n\varepsilon_0$ quantum states $|\delta_n\rangle$ and $n\varepsilon_1$ quantum states $|\eta_n\rangle$ are consumed in the security testing phase, which causes inefficiency.

The specific voting process is similar to that in the protocol proposed in Ref. [23] and thus a brief description of it is given. Denote the n voters as $N_0, N_1, \cdots, N_{n-1}$ and the m candidates as $0, 1, \cdots, m-1$. It mainly has three parts as follows.

Firstly, n quantum states in the form of $|\zeta_n\rangle$ are generated by the distribution center CA and distributed to other voters. The representative node inserts trap qubits into the sequence of qudits to be distributed to other voters for resisting the man-in-the-middle attack. After a security test, voters share n quantum states $|\zeta_n\rangle$ and each of them holds one qudit of each quantum state. By measuring the kept qudits in the computational basis, each voter gets n values as ballot boxes, which can be represented by the matrix

$$\begin{pmatrix} r_{0,0} & \cdots & r_{0,k} & \cdots & r_{0,n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ r_{j,0} & \cdots & r_{j,k} & \cdots & r_{j,n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ r_{n-1,0} & \cdots & r_{n-1,k} & \cdots & r_{n-1,n-1} \end{pmatrix}, \quad (10)$$

where $j, k \in \{0, 1, \ldots, n-1\}$ and $r_{j,k} \in \{0, 1, \ldots, l-1\}$. Note that the k-th column $\{r_{0,k}, \ldots, r_{j,k}, \ldots, r_{n-1,k}\}$ is owned by the voter N_k for $k = 0, 1, \ldots, n-1$. According to the properties of $|\zeta_n\rangle$, there is

$$\sum_{k=0}^{n-1} r_{j,k} \bmod l = 0, \quad (11)$$

where $j = 0, 1, \ldots, n-1$.

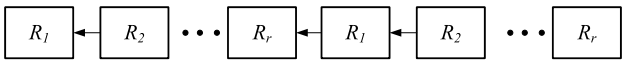

Fig. 6. Block generation is performed cyclically by representative nodes.

Secondly, the quantum state $|\eta_n\rangle$ is distributed to generate index numbers similar to the distribution of $|\zeta_n\rangle$ in the first step. By measuring the held particle in the computational basis, each voter gets a value called index number. All index numbers form $(d_0, d_1, \ldots, d_n) \in P_n^n$ and N_k uses the d_k-th ballot box for voting.

Finally, voters cast their ballots using the ballot boxes designated by their respective index numbers. N_k votes for the ballot $v_k \in \{0, 1, \ldots, l-1\}$ by adding v_k to $r_{d_k,k}$, where $[0, \cdots, m-1]$ are for positive votes, $[m, \cdots, 2m-1]$ are for negative votes, and $2m$ is for abstention. Voters renew ballot numbers $r'_{j,k}$ as

$$r'_{j,k} = \begin{cases} r_{j,k} + v_k \bmod l & \text{if } j = d_k, \\ r_{j,k} & \text{if } j \neq d_k. \end{cases} \quad (12)$$

After the polls close, all voters announce the values of their ballot boxes at the same time and each voter is given the reordered results of the votes by calculating the updated ballot boxes matrix

$$\begin{pmatrix} r'_{0,0} & \cdots & r'_{0,k} & \cdots & r'_{0,n-1} & result_0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ r'_{j,0} & \cdots & r'_{j,k} & \cdots & r'_{j,n-1} & result_j \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ r'_{n-1,0} & \cdots & r'_{n-1,k} & \cdots & r'_{n-1,n-1} & result_{n-1} \end{pmatrix}, \quad (13)$$

where $result_j = \sum_{k=0}^{n-1} r'_{j,k} \mod l$, to complete the anonymous voting. By counting the number of votes for positiveness, negativeness, and abstentions for each candidate node, the top r nodes with the most votes among the m candidate nodes become the representative nodes.

Step 2: Block production. After the representative nodes are selected, they are sorted in a random order of appearance. The blocks are generated cyclically by them as shown in Fig. 6. Let a fixed block-out time be t. When it is the turn of a representative node to work, he collects information about transactions that occur in time t, verify the correctness of them, and insert the validated transaction information into the block. If a representative node misses his working time, the block is invalidated and the transactions contained in it are carried forward to the next block. The blockchain generated by the representative nodes is the longest chain and there is very little possibility of a fork.

Step 3: Incentives. To ensure QDPoS achieving better performance, economic factors are combined with it to provide incentives for nodes. Once a representative node successfully produces a block, it gets a block bonus. Similarly, when a node successfully participates in quantum voting, it can receive some rewards, which can be in the form of some kind of blockchain transaction, such as virtual currency. But if a node violates the rules of QDPoS such as breaking quantum voting and producing wrong blocks, he will be punished by deducting

Authorized licensed use limited to: University College Dublin. Downloaded on January 14,2025 at 17:12:14 UTC from IEEE Xplore. Restrictions apply.

rewards. Incentives can make representative nodes work more actively and get the nodes more enthusiastically involved in quantum voting.

Step 4: Re-election. In order to prevent monopolies, the identities of the representative nodes are not set in stone. After the last representative node finishes the block production, all nodes can conduct new votes to select new representative nodes. Every legitimate node can become a candidate by nomination. At the same time, original representative nodes that performed operations honestly also have the opportunity to be re-elected. In addition, during the production of blocks, if a representative node is detected to have acted illegally, nodes can always conduct a new quantum voting to make it step down.

QDPoS is a consensus method mainly based on quantum voting, which can resist quantum attacks that may be encountered in classical voting. In each round of quantum voting, n quantum states $|\zeta_n\rangle$ and a quantum state $|\eta_n\rangle$ are required. Since $|\zeta_n\rangle$ contains n particles of level $2m+1$ and the generation of each particle needs $\log 2m+1$ qubits, $|\zeta_n\rangle$ requires $n\log 2m+1$ qubits to be constructed. Similar to $|\zeta_n\rangle$, $|\eta_n\rangle$ contains n particles of level n and requires $n\log n$ qubits to build. So a total of $n^2\log 2m+1+n\log n$ qubits are necessary to construct these quantum states. Similar to DPoS, QDPoS can reach consensus in a shorter time and more fairly and it consumes less computational resources compared with PoW and PoS. Especially in the quantum environment, QDPoS becomes a better choice for quantum blockchains and the designed QDPoS consensus method can be applied to the quantum blockchain to be proposed later.

IV. Quantum Blockchain Based on QDPoS

A quantum blockchain scheme is to be designed by combining the above-mentioned quantum technologies, where quantum blocks are constructed by employing quantum states and the entanglement properties between quantum states are used to link the blocks to form chains. Furthermore, quantum consensus mechanism and quantum digital signature are used to ensure the efficiency and security of quantum blockchain. Specifically, classical information is set as phases of quantum states to generate quantum blocks chained by using C^kZ gates, where k is a positive integer less than the number of all quantum blocks. The structure of the chain can be either weighted graph states or weighted hypergraph states. Each node can use the method of quantum digital signature in Ref. [26] to generate verifiable information and sends it to other nodes for verification. By QDPoS consensus method, verified messages are written to the quantum block and all nodes can add this new quantum block to their own local quantum blockchain. In the following, the structure of the quantum block and chain is described and the steps of designing a quantum blockchain scheme are given.

A. The Construction of the Quantum Block and Chain

We use the way similar to that in the scheme proposed by Banerjee *et al.* [32] to construct a quantum block. Consider a classical message M for which there exists a bijective function

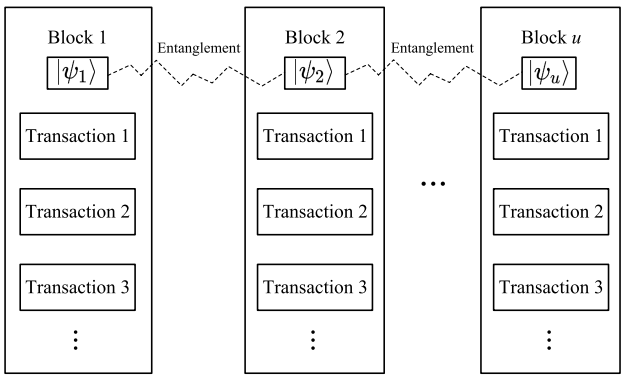

Fig. 7. Quantum blocks are linked to each other by entanglement operations.

F transforming it into an phase angle: $F(M) \longleftrightarrow \theta_M$. Then the rotation operation $R(\theta_M)$ is applied on the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ to generate

$$|\psi\rangle = R(\theta_M)\,|+\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta_M} \end{bmatrix} \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{i\theta_M}\,|1\rangle}{\sqrt{2}}, \tag{14}$$

where $\theta_M \in [0, 2\pi)$. The state $|\psi\rangle$ represents a quantum block which records the classical information M. Suppose u quantum blocks $|\psi_1\rangle,\ |\psi_2\rangle,\ \cdots,\ |\psi_u\rangle$ are

$$\begin{aligned} |\psi_1\rangle &= \frac{|0\rangle + e^{i\theta_{M_1}}\,|1\rangle}{\sqrt{2}}, \\ |\psi_2\rangle &= \frac{|0\rangle + e^{i\theta_{M_2}}\,|1\rangle}{\sqrt{2}}, \\ &\cdots \\ |\psi_u\rangle &= \frac{|0\rangle + e^{i\theta_{M_u}}\,|1\rangle}{\sqrt{2}}, \end{aligned} \tag{15}$$

where $M_1,\ M_2,\ \cdots,\ M_u$ are classical messages. For constructing a chain, quantum entanglement is used instead of the hash function to link quantum blocks together as shown in Fig. 7. Because the property of quantum block is a quantum state, classical hash values do not apply to it. Meanwhile, using quantum entanglement to build chains can solve the problem of violent cracking of hash functions by quantum computers. Two ways of generating entanglement can be used to connect quantum blocks. (a) The first way is that quantum blocks are entangled by CZ operations to form a weighted graph state. A new quantum block is added through the CZ operation with the previous quantum block as the control qubit and itself as the target qubit. The weighted graph state constructed in this way is the structure of the chain as shown in Fig. 8. For three quantum blocks $|\psi_1\rangle$, $|\psi_2\rangle$ and $|\psi_3\rangle$, they are entangled to be a chain in the form of a weighted graph state represented as

$$\begin{aligned} |\psi_{123}\rangle &= (I\otimes CZ)(CZ\otimes I)(|\psi_1\rangle\otimes|\psi_2\rangle\otimes|\psi_3\rangle) \\ &= \frac{1}{2\sqrt{2}}(|000\rangle + e^{i\theta_{M_3}}\,|001\rangle + e^{i\theta_{M_2}}\,|010\rangle \\ &\quad -e^{i\theta_{M_2+M_3}}\,|011\rangle + e^{i\theta_{M_1}}\,|100\rangle + e^{i\theta_{M_1+M_3}}\,|101\rangle \\ &\quad -e^{i\theta_{M_1+M_2}}\,|110\rangle + e^{i\theta_{M_1+M_2+M_3}}\,|111\rangle). \end{aligned} \tag{16}$$

(b) The other way is that quantum blocks are entangled by C^kZ operations to form a weighted hypergraph state [32].

Authorized licensed use limited to: University College Dublin. Downloaded on January 14,2025 at 17:12:14 UTC from IEEE Xplore. Restrictions apply.

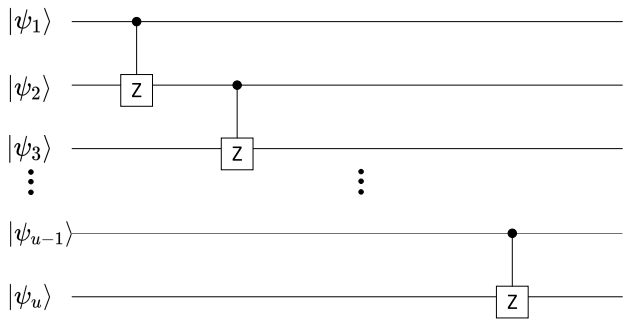

Fig. 8. Circuit diagram of a quantum blockchain using a weighted graph state with two adjacent quantum blocks linked by the CZ gate.

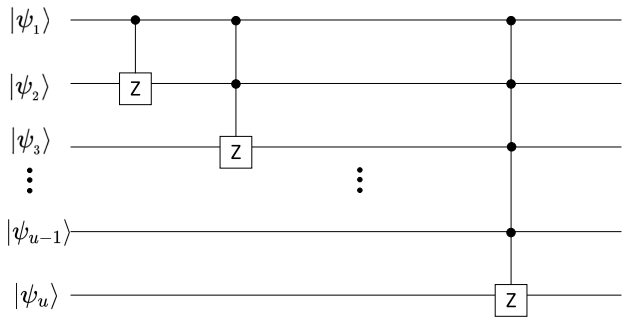

Fig. 9. Circuit diagram of a quantum blockchain using weighted hypergraph states with $k+1$ adjacent quantum blocks linked by $C^k Z$ gates, where $k = \{1, 2, \cdots, u-1\}$.

The $k+1$-th quantum block is added to the chain by the $C^k Z$ gate operation with the previous k quantum blocks as control qubits and itself as the target qubit. The chain of u quantum blocks is the weighted hypergraph state of u qubits as shown in Fig. 9. For instance, if there are three quantum blocks $|\psi_1\rangle$, $|\psi_2\rangle$ and $|\psi_3\rangle$, they are chained by entanglement in the form of a weighted hypergraph state described as

$$\begin{aligned}|\psi_{123}\rangle &= (C^2Z)(CZ \otimes I)(|\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle) \\ &= \frac{1}{2\sqrt{2}}(|000\rangle + e^{i\theta_{M_3}}|001\rangle + e^{i\theta_{M_2}}|010\rangle \\ &\quad + e^{i\theta_{M_2+M_3}}|011\rangle + e^{i\theta_{M_1}}|100\rangle + e^{i\theta_{M_1+M_3}}|101\rangle \\ &\quad - e^{i\theta_{M_1+M_2}}|110\rangle + e^{i\theta_{M_1+M_2+M_3}}|111\rangle). \end{aligned} \tag{17}$$

B. The Process of Quantum Blockchain

1) Preparation Stage: Assume that there are n nodes $N_0, N_1, \cdots, N_{n-1}$ in the quantum blockchain. Since quantum digital signature will be used, the node N_i for $i = 0, 1, \cdots, n-1$ should generate a quantum private key sk_i and the corresponding quantum public key pk_i by using a quantum one-way function $f : sk \longrightarrow |f_{sk}\rangle$ introduced in Ref. [26] several times, which can map a L-bit classical string to a quantum state of H qubits and allow L to be much greater than H. Let the security parameter be D and D L-bit classical strings are necessary to sign a bit transaction information. For a b-bit message T used for transaction, its signature is generated by repeating the above way of dealing with one bit b times. Let $sk_0, sk_1, \ldots, sk_{n-1}$ be the quantum private keys and $pk_0, pk_1, \ldots, pk_{n-1}$ be the public keys of nodes $N_0, N_1, \ldots, N_{n-1}$. The node N_i with the quantum private key sk_i can generate the message-signature pair $(T, S_i(T))$ by using the quantum digital signature method proposed in Ref. [26]. The nodes who receive $(T, S_i(T))$ can use a copy of the corresponding quantum public key pk_i to verify the signed message by means of the swap test.

Then the first round of quantum voting is conducted to select the first round of representative nodes $R_1, R_2, \ldots, R_r$ for QDPoS consensus. Nodes nominate candidates by competing with each other. Then representative nodes are elected among candidates through the improved quantum voting protocol. The quantum resources required for quantum voting are similarly allocated by CA. Representative nodes perform corresponding operations according to the rules of QDPoS.

In addition, the structure of the chain can be weighted graph state or weighted hypergraph state and the bijective function F which maps a classical message to a phase angle used in the quantum blockchain are jointly determined by all nodes.

2) Quantum Blockchain Workflow: The quantum blockchain is essentially a decentralized and distributed ledger maintained by all nodes together. Each node can make transactions in the quantum blockchain and the format of the information related to transactions is classical information. A quantum block consisting of a single qubit can record such information. The workflow of quantum blockchain is shown in Fig. 10 and it consists of four steps as follows.

Step 1: Generating and broadcasting transaction information. The node N_i generates the signature $S_i(T_i)$ of the transaction T_i with the quantum private key sk_i and broadcasts $(T_i, S_i(T_i))$ to the network.

Step 2: Verifying transaction information. The nodes who received the transaction information T_i verify the correctness and legitimacy of T_i by the corresponding quantum public key pk_i and record it.

Step 3: Implementing the proposed QDPoS consensus algorithm. The representative node R_j who is decided by the QDPoS consensus method generates the new quantum block. Assume that each representative node works for time t and R_j collects information about the transactions that occur in time t. R_j first verifies the correctness of these transactions and then adds the successfully verified transaction information to the quantum block $|\psi\rangle$. The quantum block $|\psi\rangle = \frac{|0\rangle + e^{i\theta_M}|1\rangle}{\sqrt{2}}$ is generated as

$$|\psi\rangle = R(\theta_M)|+\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta_M} \end{bmatrix} \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{i\theta_M}|1\rangle}{\sqrt{2}}, \tag{18}$$

where M contains the transaction messages that have passed verification and other related information, the angle θ_M is obtained by the bijective function F: $F(M) \longleftrightarrow \theta_M$, and $R(\theta_M)$ is a rotation operation with the angle θ_M. After the quantum block $|\psi\rangle$ is generated, R_j broadcasts the classical information θ_M related to $|\psi\rangle$ to other representative nodes. After passing the verification of more than half of representative nodes who voted in favor, R_j broadcasts θ_M to the peer-to-peer network.

Authorized licensed use limited to: University College Dublin. Downloaded on January 14,2025 at 17:12:14 UTC from IEEE Xplore. Restrictions apply.

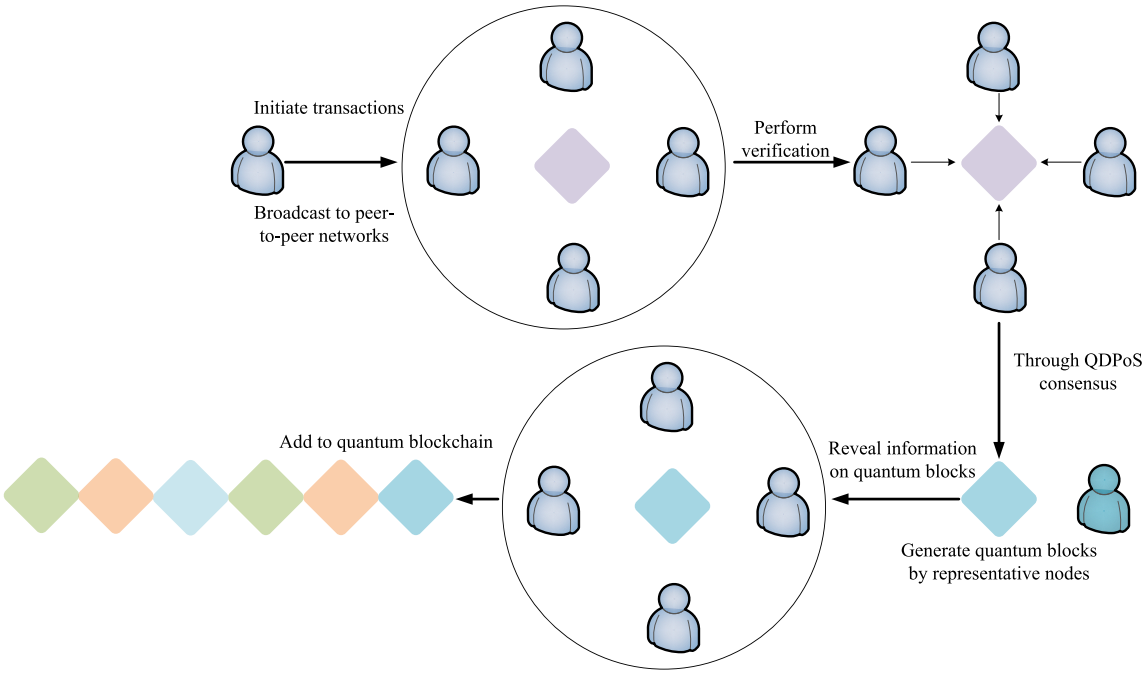

Fig. 10. Workflow of the quantum blockchain.

Step 4: Adding the new quantum block to the quantum blockchain. When the nodes receive the classical information θ_M about the new quantum block broadcasted by the representative node R_j, they can verify the correctness of the quantum block since all transaction information is publicly transparent and they are aware of the bijective function F. Then they can generate the new quantum block $|\psi\rangle$ and add it to the local quantum blockchain through quantum entanglement operations if it passes the verification. Note that the structure of the chain can be a weighted graph state or a weighted hypergraph state and it is decided jointly by all nodes in the preparation stage.

Through the quantum blockchain scheme, nodes can complete secure peer-to-peer transactions and solve the quantum computing challenges that classical blockchain schemes may encounter. There is no difference in function between quantum blockchain and classical blockchain and only the ways to implement these functions are different, such as producing quantum blocks or classical blocks, and employing quantum digital signature or classical digital signature. In the proposed quantum blockchain scheme, the QDPoS consensus method is used and it is more inclined to consortium chains. The quantum blockchain can be used as an alternative to the classic blockchain and may be applied in finance, IoT, medical and other fields which need stronger security.

V. Security Analysis and Comparisons

A. Security Analysis

In this subsection, the security of the proposed quantum blockchain scheme is analyzed in two aspects. The first aspect is the security of the structure of the quantum blockchain. Quantum blocks are the carriers of information, which are linked together by quantum entanglement to form a chain. Since the quantum blockchain is a decentralized and distributed ledger, it is crucial to guarantee the immutability of information. The second aspect of the security of the quantum blockchain lies in the unforgeability and consistency of related transactions, as there is no third party to verify the transaction and make all nodes agree on it.

Theorem 1: Untamperability of quantum blockchain. For any adversary $\mathcal{A}$ with quantum power, if he tampers with any of quantum blocks, he will be detected.

Proof: A quantum block consists of a quantum state $|\psi\rangle$ where the classical information M is related to the phase of it. Because the bijection function F is known to all nodes, each node can generate the corresponding quantum block $\frac{|0\rangle+e^{i\theta_M}|1\rangle}{\sqrt{2}}$. The chains is formed by entangling quantum blocks in the form of weighted graph states or weighted hypergraph states rather than by hashing them. If an external attacker $\mathcal{A}$ wants to tamper with the k-th quantum block, he needs to measure the quantum block to obtain information about it. Since quantum blocks are entangled with each other, measuring one of them will cause the whole chain to collapse and Eve will not get the information she wants. If an insider attacker $\mathcal{A}$ wants to carry out the attack, he needs to change the phase of the k-th quantum block through the quantum operation. But this attack is also not effective. As all quantum operations are reversible, each node can determine if a quantum block has been tampered with by measuring it. □

Theorem 2: Non-forgeability of signatures. For any quantum adversary $\mathcal{A}$, the probability that he can successfully forge a legitimate signature is negligible if n as the number of the participating nodes in the proposed quantum block chain scheme is not large enough.

Proof: Quantum digital signature methods are used to sign transaction messages and they are unnecessary to rely

Authorized licensed use limited to: University College Dublin. Downloaded on January 14,2025 at 17:12:14 UTC from IEEE Xplore. Restrictions apply.

on some difficult mathematical problems. Assume a b-bit transaction message is to be signed. Quantum private and public key pairs (sk_i, pk_i) of nodes N_i are generated by using quantum one-way functions [26], where one quantum private key $sk_i = \{k_0^i, k_1^i\}$ consists of bD-pair binary strings and each string is L bits, and the corresponding quantum public key $pk_i = \left|f_{sk_i}\right\rangle = \{|f_{sk_0^i}\rangle, |f_{sk_1^i}\rangle\}$ is a set of quantum state sequences of $2H$ qubits. According to the Holevo's theorem, at most H bits of information can be obtained by measuring a quantum state of H qubits. Considering the worst case that the quantum adversay $\mathcal{A}$ obtains n copies of quantum public key $|f_{sk}\rangle$, he can obtain at most nH bits of information about each binary string k_j^i from them, where $i \in \{0, 1, \cdots, bD\}$ and $j \in \{0, 1\}$. $\mathcal{A}$ can only guess the correct information about sk of length $E = 2^{-(L-nH)}(2bD)$. If $L - nH \gg 1$, $\mathcal{A}$ cannot recover the whole quantum private key from the E bits of information and the probability that $\mathcal{A}$ successfully forge a legitimate signature is negligible.

So it is able to prevent quantum attacks and guarantee authenticity, non-forgeability and non-repudiation of transactions. But in order to be unconditionally secure, the keys for signing transaction information are used only once and new transactions should use different keys. □

Theorem 3: Nodes with quantum computers cannot affect the fairness of the QDPoS consensus mechanism. For any quantum adversary $\mathcal{A}$, his computing power advantage does not determine the bookkeeping of blocks.

Proof: we construct a QDPoS consensus mechanism based on quantum voting which provides decentralized functionality for the quantum blockchain. Due to the current scarcity of quantum resources, the quantum capabilities of all parties are unbalanced. Nodes with powerful quantum computers have more computing power than other nodes, causing consensus mechanisms such as PoW and PoS to be inapplicable. In the QDPoS consensus mechanism, nodes do not rely on computing power, the quantum voting is crucial to achieve fairness. The security of quantum voting is based on the principle of quantum mechanics, and $\mathcal{A}$ does not use the computational advantage to get more votes. The process of distributing the quantum states required for quantum voting may be subject to attack by $\mathcal{A}$, who may try to know which candidate the node voted for by eavesdropping on the nodes' ballot boxes and index numbers. But it can be avoided by inserting trapped qubits into the distributed qudits to make attacker be unknown about the locations of the trapped qubits. In addition, $\mathcal{A}$ may attempt to use other nodes' ballot boxes and index numbers to disrupt the voting results. Each node N_k can verify their voting result by checking whether the equation $v_k = result_{d_k}$ is right. The consensus process of blockchain is carried out according to the rules of QDPoS and the right to bookkeeping of blocks is not affected by the strength of computing power. □

B. Comparisons Among Similar Quantum Blockchain Schemes

There exist few quantum blockchain schemes at present, but the ones in Refs. [30], [31], [32] are relatively better. In this part, some comparisons are made between the proposed quantum blockchain scheme and these three typical quantum blockchain schemes as shown in Table I. Firstly, in the proposed scheme, quantum digital signature is used to achieve undeniability of nodes and unforgeability of transactions. It is similar to the idea of asymmetric cryptosystem, in which the sender's signature can be verified by any people who knows the quantum public key. The sender only needs to prepare a copy of the signed transaction message and transmits a copy of the quantum public key to each participating node. Then only one-way communication is implemented $O(n^2)$ times to distribute $O(n^2)$ keys for n nodes to achieve verification. Since the quantum public key of a node distributed to other nodes is the same, nodes cannot deny what they have done. But the quantum blockchain schemes in Ref. [30] and Ref. [31] used QKD to distributes keys for each pair of nodes for verification and thus two-way communication should be implemented $O(n^2)$ times to distribution $O(n^2)$ keys. Especially, they cannot provide undeniability since the keys shared by each pair of nodes are the same.

Secondly, the QDPoS consensus method used in the proposed quantum blockchain scheme can elect representative nodes for quantum block production by quantum voting, which is more fair and more efficient than other consensus mechanisms given in Refs. [30], [31], [32]. As selecting representative nodes through a round of quantum voting with time complexity $O(n)$ can maintain the blockchain running well over a period of time, the consensus time complexity of the proposed scheme is $O(n)$, while that of other schemes are $O(n^{f+1})$, $O(n^2)$ and $O(n)$, respectively, where f is the number of faulty nodes. The scheme proposed in this paper and that given in Ref. [30] can provide Byzantine fault tolerance, while the schemes offered in Refs. [31], [32] cannot. The tolerance rates of the faulty nodes are $\frac{n}{2}$, $\frac{n}{3}$, 0, and 0, respectively. In addition, in other schemes, the nodes perform the production of blocks individually, and the blockchain system is less robust. And in the proposed scheme, as the block information broadcasted during the consensus process is classical information and no additional quantum information needs to be sent one-to-one, it is relatively faster to generate quantum blocks. While the schemes in Refs. [31], [32] need to send quantum states through quantum channels for verification and thus they consume $2n$ qubits and n qubits, seperately.

Furthermore, for the construction of quantum blocks, the proposed quantum blockchain scheme uses a quantum state $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ to generate a quantum block $\frac{|0\rangle+e^{i\theta_M}|1\rangle}{\sqrt{2}}$ by loading c-bit classical information M in the form of phase θ_M onto $|+\rangle$. M contains information of a classical block and thus a quantum block of a single qubit can realize the function of a classical block. The size of M is c which can be large enough and this is a huge improvement compared with the classical block. In Ref. [31], quantum blocks $\left|\beta_{xy}\right\rangle$ are generated by Bell states

$$\left|\beta_{xy}\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle|y\rangle + (-1)^x|1\rangle|\bar{y}\rangle), \tag{19}$$

where xy are two classical message bits and the informational amount of them is too small. In addition, the proposed scheme

Authorized licensed use limited to: University College Dublin. Downloaded on January 14,2025 at 17:12:14 UTC from IEEE Xplore. Restrictions apply.

TABLE I
COMPARISONS BETWEEN THE PROPOSED SCHEME AND OTHER QUANTUM BLOCKCHAIN SCHEMES

	The proposed scheme	The scheme in Ref. [30]	The scheme in Ref. [31]	The scheme in Ref. [32]
Communication complexity for verifying transaction messages	One-way communication performed $O(n^2)$ times	Two-way communication performed $O(n^2)$ times	Two-way communication performed $O(n^2)$ times	N/A
Undeniability of nodes	Yes	No	No	N/A
Consensus mechanism	QDPoS	Byzantine agreement	θ-protocol	Relative phase consensus
Consensus time complexity	$O(n)$	$O(n^{f+1})$	$O(n^2)$	$O(n)$
Byzantine fault tolerance	Yes ($\frac{n}{2}$)	Yes ($\frac{n}{3}$)	No(0)	No(0)
Quantum resource loss during the consensus process	No	N/A	$2n$ qubits	n qubits
Resource requirements for generating a block	1 single-qubit state $\|+\rangle$	c classical bits	1 two-qubit Bell state	1 single-qubit state $\|+\rangle$
Information volume of a single block	c bits	c bits	2 bits	c bits
The structure of the chain	Weighted graph state or Weighted hypergraph state	Classical chain	GHZ state	Weighted hypergraph state
Resisting the hashrate attacks	Yes	No	Yes	Yes

is flexible since it can use both weighted graph states and weighted hypergraph states to entangle quantum blocks to build chains. The weighted graph state and the weighted hypergraph state have their own advantages. The weighted graph state is easy to generate since only CZ operations are applied on two adjacent quantum blocks, while the generation of weighted hypergraph state requires C^kZ operations on k existing quantum blocks and a new quantum block, where k is less than the number of all quantum blocks in the quantum blockchain. But the entanglement degree of the weighted graph state is relatively lower and the risk of disconnection of the local quantum blockchain of nodes is larger compared to the weighted hypergraph state. Besides, since the information for constructing quantum blocks is publicly available, nodes can reconstruct the quantum blockchain without violating the no-cloning theorem. Finally, in the proposed quantum blockchain scheme and those in Refs. [31], [32], the use of the hash function is replaced by the entanglement between quantum blocks and thus the hashrate attack is avoided, but the scheme in Ref. [30] cannot resist the hashrate attack.

VI. AN EXAMPLE OF THE QUANTUM BLOCKCHAIN SCHEME

Here we give an example of the proposed quantum blockchain scheme. Suppose the quantum blockchain handles transactions in digital currencies. In the preparation phase, quantum keys are generated for each node. For simplicity, let the length of the transaction message T be just one bit. A node chooses a number of pairs of strings $\{k_0^i,\ k_1^i\}$ as the quantum private key, where $1 \le i \le D$ and D is the security parameter. The $\{k_0^i\}$ is used to sign a message $T = 0$, and the $\{k_1^i\}$ is used to sign a message $T = 1$. The corresponding quantum public key $\{|f_{k_0^i}\rangle,\ |f_{k_1^i}\rangle\}$ is generated through quantum one-way function f

$$\{k_0^i,\ k_1^i\} \longrightarrow \{|f_{k_0^i}\rangle,\ |f_{k_1^i}\rangle\}. \tag{20}$$

The quantum public key is distributed to the other nodes through the quantum channel. Each node can verify a single-bit message T using the following procedure:

1. A node sends the signed message $(T,\ k_T^1,\ k_T^2,\ \cdots,\ k_T^D)$ over an insecure classical channel.

2. Each recipient of the signed message generates $|f_{k_T^i}\rangle$ according to k_T^i and the one-way function f and then verifies whether it has high fidelity with the corresponding quantum state of the received public key by the swap test.

The above process can be repeated many times to realize verification of multi-bit messages. It is also possible to encode the message by performing a classical error-correcting code and then using a pair of keys for each encoded bit [26].

Then the first round of quantum voting is conducted to select current representative nodes for QDPoS consensus. An example of four nodes, three candidates and only one representative node is used to describe the process of the voting protocol. According to Eqs. (8)-(9), the four nodes share four states $|\zeta_4\rangle$ and one state $|\eta_4\rangle$, where

$$|\zeta_4\rangle = \frac{1}{7^{\frac{3}{2}}} \sum_{\sum_{k=0}^{3} j_k \bmod 7 = 0} |j_0\rangle_C |j_1\rangle_C \cdots |j_3\rangle_C \tag{21}$$

and

$$|\eta_4\rangle = \frac{1}{\sqrt{4!}} \sum_{S \in P_4^4} (-1)^{\tau(S)} |s_0\rangle |s_1\rangle \cdots |s_3\rangle . \tag{22}$$

By measuring the kept particles in the computational basis, each voter gets 4 ballot numbers and an index number. Suppose the ballot matrix held by the four nodes is

$$\begin{pmatrix} 2 & 2 & 3 & 0 \\ 0 & 6 & 0 & 1 \\ 4 & 5 & 3 & 2 \\ 1 & 4 & 1 & 1 \end{pmatrix}, \tag{23}$$

where each node holds one column of the matrix, and the index numbers (d_0, d_1, d_2, d_3) obtained by voters are $(1, 3, 0, 2)$. During the voting stage, assume the four nodes N_0, N_1, N_2, and N_3 cast votes $(v_0, v_1, v_2, v_3) = (1, 1, 0, 2)$. The voting process is shown in Table II and each voter has access to the publicly available voting results after the voting is completed. A simple calculation shows that the candidate with serial

Authorized licensed use limited to: University College Dublin. Downloaded on January 14,2025 at 17:12:14 UTC from IEEE Xplore. Restrictions apply.

TABLE II
A SIMPLE EXAMPLE OF QUANTUM VOTING WITH $n = 4$ AND $m = 3$

	N_0	N_1	N_2	N_3	results
$r'_{0,k}$	2	2	3+0	0	0
$r'_{1,k}$	0+1	6	0	1	1
$r'_{2,k}$	4	5	3	2+2	2
$r'_{3,k}$	1	4+1	1	1	1

Fig. 11. Circuit diagram for generating quantum blocks $|\psi_1\rangle$, $|\psi_2\rangle$, and $|\psi_3\rangle$, where q_0, q_1, and q_2 are initialized to $|0\rangle$.

number 1 who has the most votes becomes the representative node R_1. Then R_1 generates suitable blocks.

In three time periods t_1, t_2, t_3, suppose three quantum blocks corresponding to classical messages M_1, M_2, and M_3 are generated in the quantum blockchain through the representative nodes selected by the QDPoS consensus mechanism and the contained legitimate transactions are verified in t_1, t_2, t_3, respectively. If the representative nodes map M_1, M_2, and M_3 to $\theta_{M_1} = \frac{\pi}{16}$, $\theta_{M_2} = \frac{\pi}{4}$, and $\theta_{M_3} = \frac{\pi}{8}$ by the bijective function F, respectively, the phases of the first quantum block, the second quantum block, and the third quantum block are $\frac{\pi}{16}$, $\frac{\pi}{4}$, and $\frac{\pi}{8}$, respectively. Then the states of them are

$$
\begin{aligned}
|\psi_1\rangle &= \frac{|0\rangle + e^{i\frac{\pi}{16}}|1\rangle}{\sqrt{2}}, \\
|\psi_2\rangle &= \frac{|0\rangle + e^{i\frac{\pi}{4}}|1\rangle}{\sqrt{2}}, \\
|\psi_3\rangle &= \frac{|0\rangle + e^{i\frac{\pi}{8}}|1\rangle}{\sqrt{2}}.
\end{aligned} \tag{24}
$$

In the first time period t_1, the corresponding representative node determined by the QDPoS collects information M_1 about the transactions and maps M_1 to θ_{M_1} by the bijection function F which is broadcasted with corresponding signature to the network. Other nodes verify whether θ_{M_1} is correct and then produce a quantum block $|\psi_1\rangle$. Quantum blocks $|\psi_2\rangle$ and $|\psi_3\rangle$ are generated similarly to $|\psi_1\rangle$, as shown Fig. 11. Each generated quantum block is entangled with the previous quantum blocks to generate a local copy of the quantum blockchain. Note that if the weighted graph state is considered as the structure of the quantum blockchain, the circuit diagram of the quantum blockchain including three quantum blocks is shown in Fig. 12. And if the weighted hypergraph state is taken as the structure of the quantum blockchain, the circuit diagram of it is shown in Fig. 13. Note that all the circuit diagrams in Figs. 11, 12, and 13 are carried out on the IBM quantum computing platform and they also can be performed by employing other quantum computing platforms.

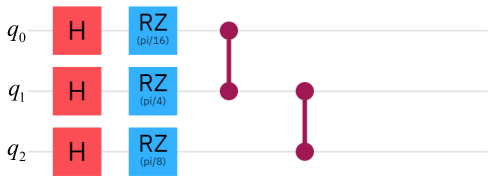

Fig. 12. Circuit diagram of a quantum blockchain scheme using weighted graph states with three qubits.

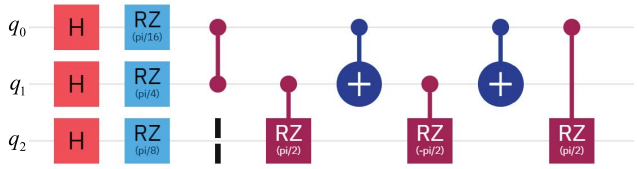

Fig. 13. Circuit diagram of a quantum blockchain scheme using weighted hypergraph states with three qubits.

TABLE III
FIDELITY OF QUANTUM BLOCKS ON REAL QUANTUM SYSTEMS

	ibm_lima	ibm_belem	ibm_nairobi
$|\psi_1\rangle$	99.12%	99.32%	99.80%
$|\psi_2\rangle$	99.12%	99.61%	98.24%
$|\psi_3\rangle$	98.83%	99.32%	99.80%

In addition, we test the fidelity of three quantum blocks by using real quantum systems such as "ibm_lima", "ibm_belem" and "ibm_nairobi" on the IBM quantum computing platform and obtained the results as shown in Table III after running 1024 times.

VII. CONCLUSION AND DISCUSSION

In this paper, we have proposed a new quantum blockchain scheme, where single quantum states are used to generate quantum blocks and the chains are formed by quantum entanglement operations. Furthermore, quantum digital signature and QDPoS consensus mechanism based on the principle of quantum mechanics are used to ensure the security of transactions. It is more efficient through the use of QDPoS consensus mechanism compared with that in other similar quantum blockchain schemes. However, the used quantum digital signature method is one-time and its security depends on the number of quantum public keys. It can be replaced with certain post-quantum digital signature schemes such as those in Refs. [44], [45], [46], [47] for further improving the efficiency of the quantum blockchain.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Decentralized Bus. Rev., White Paper, Oct. 2008. [Online]. Available: https://www.debr.io/article/21260-bitcoin-a-peer-to-peer-electronic-cash-system

[2] C. Lin, D. He, X. Huang, M. K. Khan, and K.-K.-R. Choo, "DCAP: A secure and efficient decentralized conditional anonymous payment system based on blockchain," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2440–2452, 2020.

Authorized licensed use limited to: University College Dublin. Downloaded on January 14,2025 at 17:12:14 UTC from IEEE Xplore. Restrictions apply.

[3] X. Yang, W. F. Lau, Q. Ye, M. H. Au, J. K. Liu, and J. Cheng, "Practical escrow protocol for bitcoin," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3023–3034, 2020.
[4] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117–2135, 2019.
[5] C. Catalini and J. S. Gans, "Some simple economics of the blockchain," *Commun. ACM*, vol. 63, no. 7, pp. 80–90, 2020.
[6] Y. Zhang, R. H. Deng, X. Liu, and D. Zheng, "Blockchain based efficient and robust fair payment for outsourcing services in cloud computing," *Inf. Sci.*, vol. 462, pp. 262–277, Jun. 2018.
[7] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "GDPR-compliant personal data management: A blockchain-based solution," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1746–1761, 2020.
[8] S. King and S. Nadal, "PPCoin: Peer-to-peer crypto-currency with proof-of-stake," *Self-Published Paper*, vol. 19, no. 1, pp. 1–6, Aug. 2012.
[9] D. Larimer, "Delegated proof-of-stake (DPoS)," *Bitshare Whitepaper*, vol. 81, p. 85, Apr. 2014.
[10] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi, and A. Rindos, "Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)," in *Proc. IEEE 36th Symp. Reliable Distrib. Syst. (SRDS)*, Sep. 2017, pp. 253–255.
[11] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Boca Raton, FL, USA: CRC Press, 2020.
[12] Z. Tang, X. Zhang, X. Li, and S. Zhang, "Robust image hashing with ring partition and invariant vector distance," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 200–214, Jan. 2016.
[13] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, and G. Wang, "Digital signature scheme for information non-repudiation in blockchain: A state of the art review," *EURASIP J. Wireless Commun. Netw.*, vol. 2020, no. 1, pp. 1–15, Dec. 2020.
[14] Y. Xiao, P. Zhang, and Y. Liu, "Secure and efficient multi-signature schemes for fabric: An enterprise blockchain platform," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1782–1794, 2021.
[15] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134.
[16] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, Aug. 2001.
[17] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Phys. Rev. Lett.*, vol. 79, no. 2, pp. 325–328, Jul. 1997.
[18] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Appl. Sci.*, vol. 9, no. 9, 2019, Art. no. 1788.
[19] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, Dec. 1984, pp. 175–179.
[20] Y. Ouyang, S. Tan, and J. Fitzsimons, "Quantum homomorphic encryption from quantum codes," *Phys. Rev. A, Gen. Phys.*, vol. 98, no. 4, Oct. 2018, Art. no. 042334.
[21] J. Liu, Q. Li, J. Quan, C. Wang, J. Shi, and H. Situ, "Efficient quantum homomorphic encryption scheme with flexible evaluators and its simulation," *Des., Codes Cryptogr.*, vol. 90, pp. 577–591, Mar. 2022.
[22] J. A. Vaccaro, J. Spring, and A. Chefles, "Quantum protocols for anonymous voting and surveying," *Phys. Rev. A, Gen. Phys.*, vol. 75, no. 1, 2007, Art. no. 012333.
[23] Q. Wang, C. Yu, F. Gao, H. Qi, and Q. Wen, "Self-tallying quantum anonymous voting," *Phys. Rev. A, Gen. Phys.*, vol. 94, no. 2, Aug. 2016, Art. no. 022333.
[24] Y. Li, R.-G. Zhou, R. Xu, J. Luo, and S.-X. Jiang, "A quantum mechanics-based framework for EEG signal feature extraction and classification," *IEEE Trans. Emerg. Topics Comput.*, vol. 10, no. 1, pp. 211–222, Jan. 2020.
[25] C. Li, Y. Zhang, and E. Y. Xie, "When an attacker meets a cipher-image in 2018: A year in review," *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102361.
[26] D. Gottesman and I. Chuang, "Quantum digital signatures," 2001, *arXiv:quant-ph/0105032*.
[27] Q. Li, W. H. Chan, and D.-Y. Long, "Arbitrated quantum signature scheme using bell states," *Phys. Rev. A, Gen. Phys.*, vol. 79, no. 5, 2009, Art. no. 054307.
[28] V. Dunjko, P. Wallden, and E. Andersson, "Quantum digital signatures without quantum memory," *Phys. Rev. Lett.*, vol. 112, no. 4, 2014, Art. no. 040502.
[29] K. Ikeda, "qBitcoin: A peer-to-peer quantum cash system," in *Proc. Sci. Inf. Conf.*, 2018, pp. 763–771.
[30] E. O. Kiktenko *et al.*, "Quantum-secured blockchain," *Quantum Sci. Technol.*, vol. 3, no. 3, Jul. 2018, Art. no. 035004.
[31] D. Rajan and M. Visser, "Quantum blockchain using entanglement in time," *Quantum Rep.*, vol. 1, no. 1, pp. 3–11, Apr. 2019.
[32] S. Banerjee, A. Mukherjee, and P. K. Panigrahi, "Quantum blockchain using weighted hypergraph states," *Phys. Rev. Res.*, vol. 2, no. 1, 2020, Art. no. 013322.
[33] Y.-L. Gao, X.-B. Chen, G. Xu, K.-G. Yuan, W. Liu, and Y.-X. Yang, "A novel quantum blockchain scheme base on quantum entanglement and DPoS," *Quantum Inf. Process.*, vol. 19, no. 12, pp. 1–15, Dec. 2020.
[34] A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, "Quantum computers put blockchain security at risk," *Nature*, vol. 563, no. 7732, pp. 465–467, 2018.
[35] K. Ikeda, "Security and privacy of blockchain and quantum computation," in *Blockchain Technology: Platforms, Tools and Use Cases* (Advances in Computers), vol. 111. Elsevier, 2018, pp. 199–228.
[36] J. Jogenfors, "Quantum bitcoin: An anonymous and distributed currency secured by the no-cloning theorem of quantum mechanics," 2016, *arXiv:1604.01383*.
[37] S. Singh, N. K. Rajput, V. K. Rathi, H. M. Pandey, A. K. Jaiswal, and P. Tiwari, "Securing blockchain transactions using quantum teleportation and quantum digital signature," *Neural Process. Lett.*, pp. 1–16, Jun. 2020, doi: 10.1007/s11063-020-10272-1.
[38] B. K. Behera, A. Banerjee, and P. K. Panigrahi, "Experimental realization of quantum cheque using a five-qubit quantum computer," *Quantum Inf. Process.*, vol. 16, no. 12, pp. 1–12, Dec. 2017.
[39] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2017.
[40] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, "Quantum hypergraph states," *New J. Phys.*, vol. 15, no. 11, 2013, Art. no. 113022.
[41] N. Tsimakuridze and O. Gühne, "Graph states and local unitary transformations beyond local Clifford operations," *J. Phys. A, Math. Theor.*, vol. 50, no. 19, 2017, Art. no. 195302.
[42] R. Qu, J. Wang, Z.-S. Li, and Y.-R. Bao, "Encoding hypergraphs into quantum states," *Phys. Rev. A, Gen. Phys.*, vol. 87, no. 2, Feb. 2013, Art. no. 022311.
[43] M. Hein, J. Eisert, and H. J. Briegel, "Multiparty entanglement in graph states," *Phys. Rev. A, Gen. Phys.*, vol. 69, no. 6, Jun. 2004, Art. no. 062311.
[44] D. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.
[45] Y. Yoo, R. Azarderakhsh, A. Jalali, D. Jao, and V. Soukharev, "A post-quantum digital signature scheme based on supersingular isogenies," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2017, pp. 163–181.
[46] F. Shahid and A. Khan, "Smart digital signatures (SDS): A post-quantum digital signature scheme for distributed ledgers," *Future Gener. Comput. Syst.*, vol. 111, pp. 241–253, Oct. 2020.
[47] D. Chaum, B. Cardoso, W. Carter, M. Yaksetig, and B. Aroso, "xxBFT: Linear consensus with random sampling," xx network, White Paper, Mar. 2022. [Online]. Available: https://xx.network/wp-content/uploads/2022/03/xxBFT-March-2022.pdf

Qin Li (Member, IEEE) received the bachelor's and Ph.D. degrees in computer science from Hunan Normal University, China, in 2005, and Sun Yat-sen University, China, in 2010, respectively. Since 2010, she has been with the College of Information Engineering, Xiangtan University, China, and became a Professor in 2019. Now, she is a Professor at the School of Computer Science, Xiangtan University. Her research interests include quantum computation and quantum cryptography.

Authorized licensed use limited to: University College Dublin. Downloaded on January 14,2025 at 17:12:14 UTC from IEEE Xplore. Restrictions apply.

Jiajie Wu received the bachelor's degree from the College of Information Engineering, Xiangtan University, China, in 2019, where he is currently pursuing the master's degree with the School of Computer Science. His research interests mainly include quantum computing and quantum blockchain.

Junyu Quan received the bachelor's degree from the College of Information Engineering, Xiangtan University, in 2018, where he is currently pursuing the Ph.D. degree with the School of Mathematics and Computational Science. His research interests include blind quantum computing and quantum cryptography.

Jinjing Shi (Member, IEEE) received the B.S. and Ph.D. degrees from the School of Information Science and Engineering, Central South University, Changsha, China, in 2008 and 2013, respectively. She is currently an Associate Professor with the School of Computer Science and Engineering, Central South University. Her research interests include quantum computation and quantum cryptography. She has presided over the National Natural Science Foundation Project of China and that of Hunan Province. There are 50 academic papers published in important international academic journals and conferences. She has received the Second Prize of Natural Science and the Outstanding Doctoral Dissertation of Hunan Province in 2015, and she has received the Best Paper Award in the international academic conference MSPT2011 and the Outstanding Paper Award in IEEE ICACT2012.

Shichao Zhang (Senior Member, IEEE) received the Ph.D. degree in computer science from Deakin University, Australia. He is currently a China National-Title Professor with the School of Computer Science and Technology, Central South University, China. His research interests include information quality and pattern discovery. He is a Senior Member of the IEEE Computer Society and a member of the ACM. He served/is serving as an Associate Editor for the *TKDD*, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, *KAIS*, and the IEEE INTELLIGENT INFORMATICS BULLETIN.

Authorized licensed use limited to: University College Dublin. Downloaded on January 14,2025 at 17:12:14 UTC from IEEE Xplore. Restrictions apply.