IEEE Transactions on Quantum Engineering

Received 15 June 2022; revised 1 September 2022; accepted 12 September 2022; date of publication 15 September 2022; date of current version 12 October 2022.

Digital Object Identifier 10.1109/TQE.2022.3207111

Decentralization Using Quantum Blockchain: A Theoretical Analysis

ZEBO YANG[1] (Graduate Student Member, IEEE), TARA SALMAN[2] (Member, IEEE), RAJ JAIN[1] (Life Fellow, IEEE), AND ROBERTO DI PIETRO[3] (Fellow, IEEE)

[1]Department of Computer Science and Engineering, Washington University, St. Louis, MO 63130 USA
[2]Department of Computer Science, Texas Tech University, Lubbock, TX 79409-3104 USA
[3]College of Science and Engineering, Hamad Bin Khalifa University, Doha 5825, Qatar

Corresponding author: Zebo Yang (e-mail: zebo@wustl.edu)

This work was supported in part by the NPRP under Grant #NPRP11S-0109-180242 and in part by the Qatar National Research Fund (a member of The Qatar Foundation). The findings achieved herein are solely the responsibility of the authors.

ABSTRACT Blockchain technology has been prominent recently due to its applications in cryptocurrency. Numerous decentralized blockchain applications have been possible due to blockchains' nature of distributed, secured, and peer-to-peer storage. One of its technical pillars is using public-key cryptography and hash functions, which promise a secure, pseudoanonymous, and distributed storage with nonrepudiation. This security is believed to be difficult to break with classical computational powers. However, recent advances in quantum computing have raised the possibility of breaking these algorithms with quantum computers, thus, threatening the blockchains' security. Quantum-resistant blockchains are being proposed as alternatives to resolve this issue. Some propose to replace traditional cryptography with postquantum cryptography—others base their approaches on quantum computer networks or quantum internets. Nonetheless, a new security infrastructure (e.g., access control/authentication) must be established before any of these could happen. This article provides a theoretical analysis of the quantum blockchain technologies that could be used for decentralized identity authentication. We put together a conceptual design for a quantum blockchain identity framework and give a review of the technical evidence. We investigate its essential components and feasibility, effectiveness, and limitations. Even though it currently has various limitations and challenges, we believe a decentralized perspective of quantum applications is noteworthy and likely.

INDEX TERMS Blockchains, consensus protocol, decentralized applications, identity management systems, quantum computing, quantum networks.

I. INTRODUCTION

Blockchain technology, as a peer-to-peer technique that keeps track of sequential data, and its numerous applications, e.g., cryptocurrencies, have attracted massive attention in recent years. Besides cryptocurrencies, it provides an innovative way to realize decentralized applications, which has led to many interesting research topics, such as decentralized consensus mechanisms, trustless security, cryptographical access controls, and nonrepudiation [1]. Blockchain applications span various sectors, including finance, healthcare, the Internet of Things, cybersecurity, and many others [2], [3].

Public key cryptography and hash functions are one of the blockchains' main pillars to realize secure access control and distributed data. Public key cryptography schemes generally use two keys for encryption/decryption, user authentication, and digital signatures for secure data transmissions. These schemes require public and private key pairs that can be self-generated or obtained from a public key infrastructure (PKI) consisting of a hierarchy of certificate authorities. In blockchains, they are used to authenticate network nodes. For example, Bitcoin [4] and most other existing blockchain platforms use the public-key method for elliptic curve cryptography-based digital signature algorithm (ECDSA) for user authentication and access control. Also, hash functions are used to securely "chain" the data stored in blocks by referencing each block to its previous/parent block using the previous block's hash. For example, SHA-256 is used as a hash function to chain the data blocks in Bitcoin.

Public key cryptography and hash functions are prevalently used and are secure enough against factorization attacks and brute force attacks using classical computers. This is due to the difficulty of solving large-number factorization and reversing one-way functions. However, quantum computers have provided polynomial-time solutions to solve factorization (e.g., Shor's algorithm) [5] and efficient ways to reverse one-way hash functions in $O(\sqrt{n})$ (e.g., Grover's algorithm) [6]. In addition, such algorithms can also be used to find hash collisions efficiently, which could result in data tampering in blockchains [7]. Recent articles have shown the significance of tackling potential quantum threats to classical blockchains [8], [9], [10].

To address the potential quantum threats, new classical cryptography algorithms, called postquantum cryptography, are being developed [11]. They use cryptographic primitives other than factorization, such as lattice, for public key schemes to avoid potential threats based on Shor's algorithm. Blockchains use public key schemes to secure their user accounts (public keys to generate addresses and pass codes based on private keys). If such public key schemes are endangered (e.g., pass codes can be found), user assets (e.g., cryptocurrencies) will no longer be secure. Postquantum blockchains that use postquantum public key cryptography have been developed and are claimed to be immune to quantum attacks [12]. They replace blockchains' current public key cryptography with postquantum counterparts. On the other hand, the vulnerability of hash functions is not as impactful since we can increase the hash length to resist quantum attacks (e.g., a hash collision that maps two inputs to the same hash value). However, increasing the length sacrifices performance.

Moreover, quantum blockchains that are solely (or in a hybrid manner) based on quantum computer networks (or the so-called quantum internet) are also being explored [13], [14], [15], [16], [17]. The classical data chain has been redesigned in a quantum manner by correlating quantum states over entanglements. "Unconditional security" of quantum decentralization is claimed for such quantum blockchains [16], [17].

However, quantum blockchains are still in their early phase and thus still lack sufficient research and implementation on the infrastructures. Quantum blockchain infrastructures, such as access control and user authentication, must be established before any quantum decentralization. Hence, in this article, we theoretically explore the essential components of a decentralized quantum application based on quantum blockchains.

The contributions of this article are listed as follows:

1) We provide a theoretical analysis of quantum blockchains and their use for a decentralized identity authentication application.
2) We accommodate the classical blockchain identity management with quantum advantages against the quantum threats (to classical cryptography).
3) We put together a conceptual design for a quantum blockchain identity framework (QBIF) and give a review of the related technologies.
4) We investigate the feasibility, effectiveness, and limitations of QBIF's essential components.

Even though it comes with various limitations and challenges, we believe a decentralized perspective of quantum applications is noteworthy and likely. Identity management frameworks promise to maintain users' identity information securely, and decentralized identity removes the concerns of centralization that violates user privacy [18]. Layering it to the quantum domain gets rid of the quantum threats. We believe that making blockchain quantum native and rebuilding everything from there would be an ideal way to implement quantum blockchains and their applications, but the current quantum technologies do not allow us to do that. This article analyzes the classical-to-quantum transition from a more realistic perspective by adopting existing technologies.

The rest of the article is organized as follows. Section II discusses the current technologies of quantum blockchains and blockchain-based identity. Then, in Section III, we give a pedagogical introduction to the quantum technologies that QBIF is layered on. With these two sections giving background and preliminary knowledge, in Section IV, we introduce the conceptual design of QBIF module by module. After that, in Section V, we discuss the challenges and limitations of QBIF. Finally, we give overall conclusions in Section VI.

II. BACKGROUND AND RELATED WORK

In this section, we introduce blockchains, quantum blockchains, and blockchain-based identity applications.

A. BLOCKCHAINS AND QUANTUM BLOCKCHAINS

A blockchain is a shared and immutable ledger that maintains data in the form of transactions [4]. Transactions are linked by a Merkle tree and stored in blocks chained by hash functions. A blockchain is composed of a peer-to-peer distributed network, where each node keeps a copy of a growing chain of blocks, and the network uses a consensus protocol to add new blocks and agree on the sequence of these blocks.

In general, blockchain users' (or clients') broadcasting of transactions starts a blockchain process. A new block with the latest transactions is made according to a particular consensus protocol (e.g., proof-of-work and proof-of-stake) [1], [2]. Several network nodes may compete to produce the new block for incentives in these consensus protocols. For example, in Bitcoin, the creator (called "miner") of a block that is eventually accepted as a permanent part of the chain wins the competition and is rewarded. Each new block points to a previously created block that the creator of the new block accepts. Thus, a block followed by the longest chain in Bitcoin is considered final. Other blockchains use other similar methods for consensus.

As discussed, every block has a hash value and points to its previous hash value. If one of the blocks is tampered with, all its following blocks become invalid. Blockchain nodes discard this tampered copy of the chain and keep working on the chain that the majority keeps. By adding extra data to block headers or transactions, decentralized storage can be achieved. Together with the blockchain event triggers, smart contracts [19] and decentralized applications have been widely developed.

User access control in blockchains relies on public-key cryptography. Blockchain users keep their private keys as passwords to their accounts and use their public keys as account numbers. Transactions usually include their generators' (e.g., payers in cryptocurrency) signatures, which are done using their private keys. Network nodes that produce blocks verify all the new transactions by validating the signature with the generators' public keys and discarding invalid ones.

Commonly used public-key cryptography methods [e.g., ECDSA and Rivest–Shamir–Adleman (RSA)] rely on the difficulty of factoring large numbers. It is easy to compute the product of two large numbers, but it is challenging to factorize a large number. On the other hand, the reliability of hash functions mainly depends on the difficulty of reversing a one-way function, such as SHA-256 and MD5. It is easy to compute the hash with inputs but hard to invert given the hash. Every different input generates a unique hash.

However, public-key cryptography and hash functions are exposed due to the rapid development of quantum computers. Shor's algorithm can factorize large numbers in a polynomial time [5], endangering public key cryptography. Grover's algorithm [6] and its derivatives provide methods with a high probability of finding the input to one-way functions by brute-force searches ($O(\sqrt{n})$, i.e., quadratic speedups) [17].

Postquantum blockchains and quantum blockchains have been proposed to solve these threats. Postquantum blockchains replace blockchains' current cryptography with classical postquantum cryptography [12]. For example, postquantum cryptographies have been proposed to replace ECDSA in blockchains (i.e., classical blockchains) with quantum attack-resistant methods [16], [20], [21]. Quantum-secured blockchains (i.e., hybrid blockchains) have been designed on top of quantum key distribution (QKD) networks [22], [23]. Quantum blockchains (i.e., fully quantum blockchains) rebuild the classical blockchains in the domains of quantum computing [13], [15], [16]. The notion of a quantum blockchain is generally inspired by the nonseparability of quantum entanglement. The sensitivity of data tampering (i.e., tampering transaction history in a block) is much stronger in quantum blockchains than in classical blockchains. Single tampering of a block would cause the denial of the whole chain, which indicates a higher level of security but a potential denial of service on a blockchain node [13]. Note that, by tampering, we mean tampering with the blockchain historical data, not tampering with transmission information in general, e.g., the man-in-the-middle attack. However, man-in-the-middle attacks can happen in every aspect of a classical network activity (at any communication link). For example, an attack can be implemented during a key-generation communication or any kind of communication that may leak a secret key. If a key is leaked or intercepted, the blockchain account associated with that key will be compromised. In the quantum realm, such attacks will not be applicable (c.f., QKD in Section II-C).

Furthermore, a hard fork in a blockchain is another infamous issue. It sometimes happens due to disagreements in the blockchain community (i.e., intentional hard fork). For example, some want to upgrade the current blockchain (e.g., to increase the block size limit), but others disagree. Then, a new version of the current blockchain appears and is kept by users who believe in it (i.e., it becomes a hard fork). On the other hand, a hard fork happening due to technical problems (i.e., accidental hard fork) is rare because it will eventually be resolved by the consensus mechanism (i.e., the majority choosing the longer chain after some subsequent blocks being produced). Hence, a typical consensus algorithm can address it regardless of whether it is a quantum or classical blockchain.

B. BLOCKCHAIN-BASED IDENTITY APPLICATIONS

Decentralized identity management has been one of the most prevalent applications of blockchains [24]. In the current internet, we have imperfect systems for digital identities that are kept in centralized storage. Centralized institutions or companies must be trusted to maintain the authority of identity authentication. Centralized identity violates user privacy and might suffer from single-point-of-failure along with many other centralization challenges. One data breach would cause the leak of all confidential information. Also, user information could be manipulated by the centralized entity for its own interests.

Blockchain-based identity management has been proposed to tackle the above issues [18], [25], [26], [27]. Every network node has the same source of truth to follow in a blockchain-based application. It replaces the centralized entity and provides flexible identity authentication. Digital identities are created as digital watermarks that are assigned to transactions. With a smart contract, such identities could be used as authentication methods for different purposes (e.g., financial and online activities).

There are usually three roles in blockchain-based identity management: owners, issuers, and verifiers. Issuers are trusted parties (e.g., local governments and companies). They can issue credentials (e.g., personal IDs and user profiles in an application) for users (i.e., owners). Owners keep the credentials to themselves and only provide them to third-party entities (i.e., verifiers) to prove their statements (e.g., age and ownership). Actual user credentials are not stored on blockchains. Only user statements' attestations (i.e., proofs) are kept on blockchains. For example, the proof of a user's date of birth may be stored on blockchains instead of the

actual date of birth. When the user provides the date of birth and the proof, verifiers validate the issuer's signature and decide the genuineness of the user-provided data.

Blockchain-based identity applications have been prevalent for years. For example, Bitnation [28], a blockchain-based borderless voluntary nation project, has been developed to reclaim the sovereignty of identity information and governance services and has been working toward the vision of world citizenship by registering identity information on the global blockchain. ConsenSys [29] has provided decentralized software services and applications. It has created a blockchain-based identity system that maintains decentralized identifiers (DIDs) for people, organizations, and objects on the blockchain platform Ethereum [19]. Startups and big companies also have proposed many blockchain-based identity applications, such as Onename [30], ShoCard [31], and Ana [32]. They used public blockchains to keep track of users' identity attestations, which were claimed to be invulnerable and easy to use. Moreover, to leverage biometric authentications for blockchain approaches, research has accentuated mobile hardware performance, such as energy consumption and computational delay [33], [34].

Even though blockchain-based identity approaches still rely on the trust we hold in the identity issuers, which may escalate into a circular trust problem when some of the issuers are compromised, we believe decentralization does, to a certain extent, resolve the centralized ownership of personal identities. For example, companies and organizations will no longer own their users' or customers' personal information. They only know if their users satisfy a particular requirement. One can choose only to reveal enough amount of their identity attributes for verification. In other words, decentralization can maximize the need to preserve the users' or customers' privacy.

C. RELATED WORK

Quantum decentralization has been discussed for years since the vision of quantum networks arose. QKD has been developed using hybrid quantum-classical networks, based on which decentralized quantum approaches (e.g., quantum blockchains) have been developed. For example, a data transmission protocol based on BB84, the first QKD protocol, and distributed ledgers has been proposed [35] to maximize the security of key transmission. Quantum computing naturally avoids some classical attacks without extra effort. For instance, in [36], a decentralized quantum cash system, qBitcoin, has been proposed based on quantum teleportation, which naturally prevents double-spend attacks. In [37], the authors propose a quantum blockchain scheme with the concept of a quantum coin based on quantum entanglement, no-cloning theorem, and a delegated proof-of-stake consensus protocol. In [38], a decentralized base-graph routing protocol has been defined based on quantum repeater networks. It allows finding the shortest paths in quantum networks using only the local knowledge of the network nodes. Other methods of adapting quantum technologies to different blockchain components and their advantages in a quantum setting have also been explored [15], [16], [17], [39].

There are various quantum approaches to achieving genuine authentication, such as quantum fingerprinting [40] and single-photon authentication [41]. An authenticator can determine whether a quantum identity matches a real one in multiple ways. For example, the quantum fingerprint is analogous to the classical digital fingerprint that associates a long string (an original string) with a much shorter string (its fingerprint), such that any two different long strings can be distinguished by only comparing their fingerprints.

However, there is no existing research on authentication applications based on quantum blockchain technology. As quantum computers are threatening the classical approaches, these applications need a way to adapt to the new challenges in the quantum era. Access control and authentication issues should be solved before decentralized quantum applications can be achieved. This article explores the feasibility of migrating the classical blockchain-based identity framework to quantum blockchains and proposes a conceptual design.

III. PRELIMINARIES

In this section, we introduce and review the preliminaries about the technologies that QBIF is based on. Table I gives the common symbols used in this article.

A. QUANTUM STATES AND THEIR OPERATIONS

A quantum bit (qubit) is the elementary unit of quantum information analogous to a bit in classical computers. While a bit has an exact value of either 0 or 1, a qubit could be in a linear superposition of both values. A qubit is usually expressed as a linear combination of $|0\rangle$ and $|1\rangle$ with their corresponding amplitudes/possibilities (or a unit vector in a complex Hilbert space)

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = (\alpha, \beta)^{\mathsf{T}} \tag{1}$$

where α and β are the amplitudes of $|0\rangle$ and $|1\rangle$. They suffice if $|\alpha|^2 + |\beta|^2 = 1$. $|\alpha|^2$ and $|\beta|^2$ are the probabilities that $|\psi\rangle$ will be measured as $|0\rangle$ or $|1\rangle$, respectively. A quantum state can be expressed with a single qubit or multiple qubits. $|0\rangle$ or $|1\rangle$ are the basis states in the computational basis. Each state preserves a probability distribution of all the measurement outcomes. For example, a 2-qubit state can be expressed as $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$.

Quantum gates do operations on quantum states. Quantum gates to quantum states are like Boolean operators (bitwise operators) to bit strings. Quantum states are mathematically expressed as complex vectors (e.g., $|0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$) and quantum gates are expressed as complex matrices (e.g., the Pauli gates X, Y, Z). It has been proven that any quantum gate can be expressed as a weighted sum of the Pauli gates (X, Y, Z), which is a common form to express gates. Assume every initial qubit is in the state of $|0\rangle$. Applying X gate

TABLE I Symbols in This Article

Symbol	Meaning
$\|\psi\rangle$	We use a Greek letter inside the bracket notation to represent a quantum state. A quantum state could be multiple qubits or one qubit (e.g., $\|\psi\rangle = \|00\rangle$).
X, Y, Z, I	The Pauli gates (the basis gates commonly used for quantum operations) and the identity gate I. Quantum gates can be expressed as complex matrices. $X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, Y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}, Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, I = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$. A symbol in a rectangle represents a gate in a quantum circuit (see Fig. 1 for examples).
CX	A controlled-not gate. It applies X gate to the target qubit if the control qubit is in state $\|1\rangle$. In a quantum circuit, it is represented by a dot connecting an X gate (see Fig. 1). The qubit associated with the dot is the control qubit. The qubit with the X gate is the target qubit.
$L, D, M, \ldots$	Quantum operations, including quantum circuits, oracles, and measurements (M), are represented as uppercase italic letters. A measurement of a quantum state yields a classical result.
$L_\varphi\|0^{\otimes n}\rangle$	A quantum circuit used to prepare a quantum state with 100% amplitude on a classical sequence of bits ψ. (e.g., $L_{10}\|00\rangle = (X \otimes I)\|00\rangle = \|10\rangle$). A quantum circuit is a sequence of quantum logic gates (e.g., Pauli gates) to operate on quantum states, analogous to classical logic gates for classical digital circuits.
$U_f\|x\rangle$	An oracle (or a quantum transformation). An oracle is a function to transform one quantum state into another, often a "black box" function. The subscript f represents a classical function $f(x)$: $\{0,1\}^n \rightarrow \{0,1\}^m$. (e.g., the constant oracle and the balanced oracle in Deutsch-Jozsa Algorithm [42], where $m = 1$). Note that in a quantum system, applying a function to a state is simply the matrix multiplication of the function (a matrix, e.g., U_f) and the state (a vector, e.g., $\|x\rangle$), so we usually just write $U_f\|x\rangle$ instead of $U_f(\|x\rangle)$.
$\|f(\psi, \rho)\rangle$	A quantum state consisting of the classical output of f with the inputs of ψ and ρ.
$\alpha\|0\rangle$, $\gamma\|00\rangle$	A quantum state part with its amplitude. In general, the measurements of quantum states are probabilistic. The square of the coefficient (amplitude) indicates the probability of the measurement result being the bits inside that bracket (e.g., 0 or 00). Note that these two symbols are not complete unless $\alpha = 1$ and $\gamma = 1$. For $\alpha\|0\rangle$, the probability of the measurement result being 0 is α^2. For $\gamma\|00\rangle$, the probability of the measurement result (two qubits) being 00 is γ^2. If all the possible measurement results are concatenated by "+" signs (e.g., $\alpha\|00\rangle + \beta\|01\rangle + \gamma\|10\rangle + \delta\|11\rangle$), all probabilities would be listed in the equation and $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 1$.

to the second qubit of a 2-qubit state can be expressed as $IX|\psi\rangle = IX|00\rangle = |01\rangle$. Operations between quantum states and gates are matrix multiplication. For example, applying X gate to $|0\rangle$ can be expressed as the matrix multiplication of X and state vector $|0\rangle$: $X|0\rangle = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \begin{pmatrix}0\\ 1\end{pmatrix} = |1\rangle$. Operations between gates and gates (or states and states) are tensor products. For example, $|0\rangle \otimes |1\rangle = \begin{pmatrix}1\\ 0\end{pmatrix} \otimes \begin{pmatrix}0\\ 1\end{pmatrix} = (01, 00)^\intercal = |01\rangle$. Note that, for simplicity, these notations are equivalent: $|b_1\rangle \otimes |b_2\rangle = |b_1 b_2\rangle$.

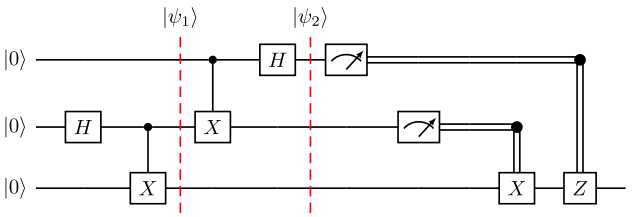


FIGURE 1. Quantum teleportation circuit.

A quantum circuit is a complete operation for a particular purpose, which usually contains a sequence of quantum gates and measurement operators. Fig. 1 shows an example quantum circuit that achieves quantum teleportation with three qubits. Solid lines are quantum wires and double lines are classical wires. H is a quantum gate called Hadamard that maps the basis states (i.e., $|0\rangle$ and $|1\rangle$ considering one qubit) to uniform superposition. A uniform superposition describes a state when it has evenly distributed amplitudes on all its possible terms (e.g., considering one qubit in (1), $\alpha = \frac{1}{\sqrt{2}}$ and $\beta = \frac{1}{\sqrt{2}}$). A meter in a rectangle (the two rectangles after $|\psi_2\rangle$ in Fig. 1) represents a measurement operation. X and Z with classical wires (on the right of Fig. 1) are classically controlled gates that use classical bits (measurement results of the top and middle qubits) as control bits to determine whether to apply the X or Z gate to the bottom qubit.

B. QUANTUM TELEPORTATION AND NETWORKS

The information encoded in a quantum state can be transmitted (actually teleported) to a remote party through entanglement. Entanglement is a quantum effect in which qubits are intrinsically linked even when long distances separate them. This kind of information transmission is called quantum teleportation.

It is called teleportation because photons are not really transmitted in this process. Still, the information is received. Unfortunately, the information at the sender's side is destroyed after the process. For example, for teleportation from Alice (the sender) to Bob (the receiver), only the state amplitudes are shuttled to Bob's state from Alice's. Alice's state information is destroyed (original amplitudes are lost) after the teleportation due to a measurement in the process. The process of quantum teleportation can be simply described as follows (together with Fig. 1):

1) Before the transmission, Alice and Bob create an entangled qubit pair together, either through a third party or themselves (i.e., operations before $|\psi_1\rangle$ in Fig. 1 creates an entangled pair for the middle and bottom states). Alice and Bob each take one qubit from the pair. Suppose Alice takes the middle qubit and Bob takes the bottom qubit. The top qubit represents the state that Alice wants to transmit. Note that the top qubit can be in any arbitrary unknown state.

2) Alice performs the controlled-not gate CX and H gates to her two qubits, as shown in Fig. 1 (between $|\psi_1\rangle$ and $|\psi_2\rangle$).
3) Alice measures her two states (the 2 m symbols after $|\psi_2\rangle$ in Fig. 1).
4) After measurement, Alice sends her results to Bob over a classical communication channel (the double lines in Fig. 1).
5) Bob then chooses to perform X or Z gates (or not) according to Alice's results to transform his qubit to the state that the top qubit was in. For example, Bob should apply X gate to his qubit (the bottom qubit) if the measurement result of Alice's middle qubit is one; otherwise, do nothing. Similarly, he should apply Z gate to his qubit if the measurement result of the Alice's top qubit is one. After these operations, the bottom quit will have the same amplitudes that the top qubit was in.

Current quantum communication and networks are mostly based on quantum teleportation. Recent articles have shown teleportation of quantum states with over 90% fidelity [43]. Fidelity describes the quality of teleportation, that is, how close the teleported qubit is to the original. There are also other researches enabling quantum state transmission. For example, Bennett et al. [44] proposed a quantum communication method called remote state preparation (RSP) based on quantum teleportation. The communication of RSP encodes one bit per qubit, by which a transmission of quantum information (a known state transmission) is realizable. However, Alice and Bob can also communicate over classical channels and remake the state at Bob's side directly if they want to transmit a known state. Even though robust quantum teleportation implementations are still under exploration, they inspire the vision of a quantum network and the quantum internet. Furthermore, in literature, a network constituted by QKD is also envisioned as an early stage of a quantum network.

It is worth noting that a peer-to-peer quantum network is assumed in almost all quantum blockchain discussions, including this article. In other words, a private (direct or indirect) quantum channel is assumed to be established between all pairs of the network nodes. Such assumptions have been commonly used as a way of reasoning for quantum networks and protocols [13], [45].

C. QUANTUM PKI

A user in a PKI has two types of keys: a public key that can be shared with anyone and a private key that is only kept by the user. The public key and private key are always in a pair. A public key can be used to encrypt a message, and only the corresponding private key can be used to decrypt it. For example, when Alice wants to send a secret message to Bob, Alice can use Bob's public key to encrypt the message and send it to him. Then, only Bob, who has the private key, can decrypt the message and see the plain text. Moreover, a private key can also be used to sign a message for nonrepudiation. For example, when Alice wants to prove that she is the sender of a message, she uses her private key to sign the message before publishing it. Then, anyone with Alice's public key can verify the source of the message by matching it.

PKI is widely used to authenticate network activities (e.g., SSH, HTTPS, blockchains, and digital identities). For identity management, it is used to generate a unique digital identity for a user by binding the user information (e.g., username and ID) with a public key. The binding is usually established by a certificate authority (CA) through the registration or sign-up process. Moreover, by signing with the user's private key, a user can prove the ownership of a message. By signing with a CA's private key, a CA can issue a statement (e.g., an attestation about an identity).

Technically, PKI is based on one-way functions, typically trapdoor functions. A trapdoor function, say, $f(x)$, is a function that, when given $f(x)$ and the secret s, it is easy to calculate the variable x. Without the secret s, it would be extremely difficult or impossible to get x. RSA is one well-known example that is based on trapdoor functions. Since the classical trapdoor functions are endangered by the development of quantum computers and algorithms (e.g., Shor's algorithm [5] and Grover's algorithm [6]), quantum-enhanced trapdoor functions have been proposed, which led to the development of quantum PKIs. They use different types of keys by design (e.g., quantum keys in the form of quantum states or classical keys that consist of classical sequences of bits).

Either with quantum keys or classical keys, the encryption and signature schemes for quantum states enable quantum PKIs. For example, in [46], quantum keys based on a quantum one-time pad are used to encrypt quantum states. Moreover, a symmetric-key encryption scheme (where the keys for encryption and decryption are the same) for quantum states (called "private quantum channels") has been developed by using a preshared single use secret key (also referred to as one-time pad) [47]. It constructs a private communication of quantum states on an insecure one-way quantum channel (using a $2n$-bit classical key to securely transmit n qubits) [47]. Such private channels enable asymmetric-key encryption and, thus, quantum PKIs. For instance, in [22], a one-way quantum identity authentication has been developed to encrypt quantum states with classical keys. In [48], public-key encryption and authentication have been developed using quantum public and classical private keys.

Here, we briefly review the quantum PKI schemes presented in [48] and [49] for quantum-state encryption, signature, and authentication. The notations introduced here will be reused for our conceptual design of QBIF presented in Section IV. The schemes are based on trapdoor one-way quantum transformations (OWQT) [48], [49]. Trapdoor OWQT is a quantum variant of a classical trapdoor function. The following paragraphs explain how the public and private

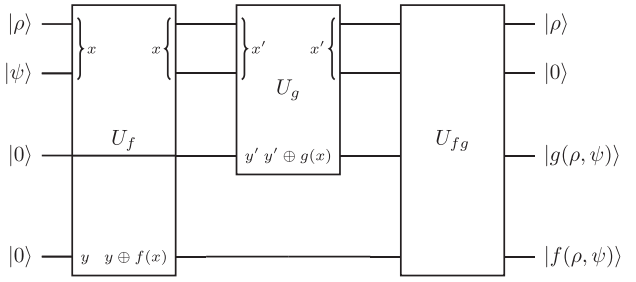


FIGURE 2. General quantum circuit for a trapdoor OWQT.

keys are made based on a trapdoor OWQT and how they are used for quantum encryption, signature, and authentication.

Public-key encryption: The definition of the trapdoor OWQT U_{OWQT} [49] can be represented as (see Fig. 2)

$$U_{\text{OWQT}}(|\rho\rangle\ |\psi\rangle\ |0\rangle\ |0\rangle) = |\rho\rangle\ |0\rangle\ |g(\psi,\rho)\rangle\ |f(\psi,\rho)\rangle \tag{2}$$

where $f(\psi, \rho)$ is a classical trapdoor one-way function with a random parameter ρ. $g(\psi, \rho)$ is another classical function. $|0\rangle$ is an initial qubit. Particularly, $f(\psi, \rho)$, $g(\psi, \rho)$, and ρ constitute a further trapdoor function as a whole, say, $h(\psi, \rho)$ [49]. $h(\psi, \rho)$ is then used to implement the quantum trapdoor OWQT U_{OWQT}. $h(\psi, \rho)$ should satisfy following conditions.

1) Easy-to-operate: Given a random parameter ρ as the trapdoor of $f(\psi, \rho)$ and $g(\psi, \rho)$, both $f(\psi, \rho)$ and $g(\psi, \rho)$ can be computed efficiently.
2) Hard-to-invert: Given the values of $f(\psi, \rho)$ and $g(\psi, \rho)$, both ψ and ρ cannot be efficiently computed.
3) Easy-to-invert with the trapdoor: There exists a trapdoor (secret information) s for the trapdoor function (the trapdoor OWQT U_{OWQT}). Given the trapdoor s, the message ψ can be efficiently computed from $f(\psi, \rho)$ and $g(\psi, \rho)$, and ρ can be efficiently computed from ψ, $f(\psi, \rho)$ and $g(\psi, \rho)$.

In other words, with secret s, it is easy to compute ψ from (2) but extremely difficult otherwise (i.e., one-way function).

Suppose we have found such function $h(\psi, \rho)$ and we now want to use it to implement the trapdoor OWQT U_{OWQT} as a quantum circuit. As shown in Fig. 2, we can implement it by translating $f(\psi, \rho)$ and $g(\psi, \rho)$ to three oracles U_f, U_g , and U_{fg} [49]. By cascading the three oracles, we get the quantum circuit for the trapdoor OWQT U_{OWQT}.

With the trapdoor function OWQT U_{OWQT}, the functions f and g are public. They can be prepared by the receiver so that only the receiver has the trapdoor s. Thus, the functions of f and g can be considered as the receiver's public key (or the tools to create public keys) and the trapdoor s as the receiver's private key. With these key generation processes, encryption and decryption of a quantum state $|\psi\rangle$ can be done as follows.

1) Bob finds a trapdoor function h and announces its components f and g as a public key. He keeps the trapdoor s to himself.
2) Alice wants to send an encrypted quantum message $|\psi\rangle$ that only Bob can read. She generates a U_{OWQT} according to Bob's public key.
3) Alice adds the parameter ρ and two initial qubits to $|\psi\rangle$ and gets $|\rho\rangle|\psi\rangle|0\rangle|0\rangle$.
4) Alice encrypts $|\rho\rangle|\psi\rangle|0\rangle|0\rangle$ by the U_{OWQT} (2) and obtains the ciphertext $|\rho\rangle|0\rangle|g(\psi,\rho)\rangle\ |f(\psi,\rho)\rangle$.
5) Alice sends the ciphertext to Bob.
6) Bob decrypts the ciphertext with s.

There are two cases of decryption [49]. Here, we directly show the decryption transformation as

$$D_{fg}(|s\rangle\,|0\rangle|0\rangle\ \ |g(\psi,\rho)\rangle\ |f(\psi,\rho)\rangle) = |s\rangle|\rho\rangle|\psi\rangle|0\rangle|0\rangle. \tag{3}$$

Signature: Even though we have the public key and private key pair, the quantum digital signature is unlike the classical digital signature. Classically, we can sign a message and send it out. Anyone with our public key can verify the message's source without our intervention. However, the quantum signature process introduced here is an interactive digital signature protocol.

Suppose Alice has a trapdoor function h , consisting of f and g (2). Here, we represent the variables as bit strings: $h(\{0,\ 1\}^{k+l}) = \{0,\ 1\}^{k'+l'}$, where $\{0,\ 1\}^{k+l}$ is a bit string of length $k + l$ with $\rho_1 \in \{0,\ 1\}^k$ (k bits) and $\rho_2 \in \{0,\ 1\}^l$ (l bits). Similarly, $\{0,\ 1\}^{k'+l'}$ consists of $\rho_{\text{r}} \in \{0,\ 1\}^{k'}$ and $\rho_{\text{s}} \in \{0,\ 1\}^{l'}$. That is

$$h(\{\rho_1, \rho_2\}) = \{\rho_r, \rho_s\} \tag{4}$$

where {a, b} denotes the concatenation of 2-bit strings, a and b. As discussed, h can be considered a public key. In this case, Alice has the private key (the trapdoor, say, s_h). The process to sign $|\psi\rangle$ and verify the signature is as follows:

1) Bob generates $\rho_{\text{r}} \in \{0, 1\}^{k'}$ randomly.
2) Alice generates $\rho_{\text{s}} \in \{0, 1\}^{l'}$ randomly and receives ρ_{r} from Bob. Now, Alice has ρ_{r}, and ρ_{s} and the trapdoor s_h. These can be used to compute the inverse of h: $h^{-1}(\rho_r, \rho_s) = (\rho_1,\ \rho_2)$. Alice then signs the quantum message $|\psi\rangle$ with ρ_1 and function h (i.e., prepared as U_h) as follows and sends it:

$$U_h|\psi\rangle|0^{\otimes(k'+l')}\rangle = |\psi\rangle\ |h(\{\psi,\ \rho_1\})\rangle \tag{5}$$

where $|0^{\otimes(k'+l')}\rangle$ denotes a state prepared with $k' + l'$ number of $|0\rangle$. For example, $|0^{\otimes 3}\rangle$ is short for $|000\rangle$.

1) Bob notifies Alice of the receipt of the quantum message.
2) Alice announces ρ_1 and ρ_2.
3) To verify the signature, Bob computes $h(\rho_1, \rho_2)$ (h is public) and checks if the first k' bits (of $\{0, 1\}^{k'+l'}$) are ρ_r. If yes, it proves Alice has the trapdoor s_h of h. Bob then performs the transformation as follows to obtain the message (h, ψ and ρ_1 are known to Bob by this step):

$$|\psi\rangle\ |h(\psi,\ \rho_1)\rangle \rightarrow |\psi\rangle\ |0^{\otimes(k'+l')}\rangle. \tag{6}$$

Finally, Bob accepts the signature only if the last $k' + l'$ qubits are all in state $|0\rangle$ (h belongs to Alice). Any signature that uses h to generate $|h(\psi, \rho_1)\rangle$ without the interactive process would be invalid. Note that this signature protocol does not support multiple verifications. The signed quantum state $|\psi\rangle\ |h(\psi, \rho_1)\rangle$ is invalid after the quantum message $|\psi\rangle$ is extracted. Therefore, this kind of signature can only be validated once. However, it is possible to obtain a local copy of the signed quantum state (a known state) [50]. The verification then only invalidates the local copy.

Usage: It is worth noting that to construct a complete user account, the quantum PKI is used differently in quantum blockchains than in classical computing. The access control in quantum blockchains (i.e., ownership of an on-chain state) is assured by interactive signatures on the index of an on-chain state (Section IV). Nonetheless, it is also important for the processes of identity attestation and authentication of QBIF (Section IV). There are many more researches on quantum PKI [46], [47], [48], [49]. For simplicity, (2), (3), (5), and (6) are used in this article to, respectively, represent quantum public-key encryption, decryption, quantum signature, and signature verification.

D. CHAIN OF QUANTUM STATES

A quantum blockchain can be constructed by a chain of nontempering and traceable quantum states. Based on quantum entanglement in time, we briefly introduce the scheme of quantum blockchains in [13] as an example. Note that this is a highly simplified version of the classical blockchain. One quantum state constitutes one block. In other words, this design assumes one transaction per block.

Before going to the chain of quantum states, we briefly explain quantum entanglement. The notion of a temper-free chain is inspired by the nonseparability of a quantum system (entanglement). Quantum entanglement in time can be viewed as a temporal quantum effect, where states are interdependent across time.

If two qubits are entangled, their measurement outcomes are correlated. If we measure one of the qubits, the other qubit instantly collapses into a definite state and would yield a correlated outcome. For example, the entanglement of the Bell states $|x\rangle$ and $|y\rangle$ may be such that the measurement result of $|x\rangle$ is exactly the same as the measurement result of $|y\rangle$. The measurement outcome of them is random, either both being 0 ($|00\rangle$) or both being 1 ($|11\rangle$). Each outcome has a 50% chance

$$|\psi\rangle = |xy\rangle = \frac{|00\rangle\ +\ |11\rangle}{\sqrt{2}}. \tag{7}$$

It is also possible for two Bell states $|x\rangle$ and $|y\rangle$ to be entangled such that the measurement result has a 50:50 chance of being $|01\rangle$ or $|10\rangle$.

Multipartite Greenberger–Horne–Zeilinger (GHZ) states generalize the qubit entanglement to achieve multiqubit entanglement, in which all the involved states are entangled with each other [51], [52].

Going back to the chain of quantum states, multiqubit entangled states can be recursively added into a growing chain in chronological order by entanglements in time [13], [53]. This chain of quantum states can be used to constitute a primitive quantum blockchain. For simplicity, a 2-bit string b_1b_2 is used here to represent the data in a block (it can be extended to larger bit strings by multiqubit entanglement, but still, it depends on the maximum qubit a quantum computer can support). Here, we prepare them into a temporal Bell state

$$|\psi_{b1b2}\rangle = \frac{|0\rangle\ |b_2\rangle\ +\ (-1)^{b_1}\ |1\rangle\ |\overline{b_2}\rangle}{\sqrt{2}} \tag{8}$$

where $|\bar{b}\rangle$ is the negation of b. Now, we can create the next temporal Bell state (next block) entangled in time with this state. These two Bell states do not actually coexist, but the second Bell state is correlated with the first one (i.e., the current state is correlated with its previous existing state). Such states were physically generated in the experiment introduced in [53]. Adding subsequent states to them forms a chain of Bell states in chronological order.

Now, we add timestamps. A delay line of time T is applied to each Bell state's creation. Each state is marked by its creation time, which becomes the block's timestamp. Let the creation time of the first Bell state (genesis block) be $t = 0$ and the time of the next state (next block) be $t = T$. The genesis block and the next block can be fused into a four-photon GHZ state

$$|\psi_{b1b2}\rangle^{0,T} = \frac{|0\rangle^0\ |b_2\rangle^T\ +\ (-1)^{b_1}\ |1\rangle^0\ |\overline{b_2}\rangle^T}{\sqrt{2}} \tag{9}$$

where 0 is the genesis block's timestamp and T is the second block's timestamp. Recursively, the blocks become a chain of entangled states (a nontempering and traceable history of a state). At $t \in \{0, T, 2T, \ldots, nT\}$, the chain of quantum states can be represented as

$$\begin{aligned}
&|\psi_{b_1b_2\ldots b_{2n}}\rangle^{0,T,T,2T,2T,3T\cdots,(n-1)T,(n-1)T,nT} \\
&\quad= \frac{1}{\sqrt{2}}(|0\rangle^0\ |\psi_{b_2}\rangle^T\ |\psi_{b_3}\rangle^T\ |\psi_{b_4}\rangle^{2T} \\
&\qquad\cdots\ |\psi_{b_{2n-1}}\rangle^{(n-1)T}\ |\psi_{b_{2n}}\rangle^{nT} \\
&\qquad+ (-1)^{b_1}|1\rangle^0|\overline{\psi_{b_2}}\rangle^T|\overline{\psi_{b_3}}\rangle^T|\overline{\psi_{b_4}}\rangle^{2T} \\
&\qquad\cdots|\overline{\psi_{b_{2n-1}}}\rangle^{(n-1)T}|\overline{\psi_{b_{2n}}}\rangle^{nT}).
\end{aligned} \tag{10}$$

Each pair of $|\psi_{b_{2i-1}}\rangle^{(i-1)T}|\psi_{b_{2i}}\rangle^{iT}$, $i \in \{2, 3, \ldots, 2n\}$, $b_i \in \{01\}$ is a block. $b_{2i-1}b_{2i}$ is the 2-bit data in a block. The superscripts iT represent the block timestamps. For example, suppose the first two blocks contain bit strings 00 and 10, and the first and second blocks are $|\psi_{00}\rangle^{0,T}$ and $|\psi_{10}\rangle^{T,2T}$, respectively. With two blocks, the chain is $|\psi_{0010}\rangle^{0,T,T,2T}$. Adding a third block with value 11 produces $|\psi_{001011}\rangle^{0,T,T,2T,2T,3T}$.

It is worth noting that entanglement in time is distinct from the more commonly used space-based entanglement [54] in

IEEE Transactions on Quantum Engineering

which photons in different locations are entangled. The entanglement in time can be viewed as a quantum networked time machine [13].

Besides using GHZ states, quantum blockchains with other kinds of states have also been experimented with. For example, Banerjee et al. [55] created a chain of quantum states using multiparty entanglement of quantum weighted hypergraph states. Bennet and Daryanoosh [56] proposed a quantum-enabled blockchain architecture using quantum information encoded in light (quantum states of light). Theoretically, the chain of hypergraph states or quantum states of light can also be used in place of the chain of GHZ states and become the data structure of a quantum blockchain using entanglement in time.

Obviously, currently implementable block size and potential chain size are not comparable with the classical blockchains. However, as quantum technologies develop, we believe quantum blockchains can be extended. More limitations and challenges of quantum decentralization are introduced in Section V.

E. PRIMITIVE CONSENSUS

In a quantum blockchain, each blockchain node hosts a copy of the chain of quantum states represented in (10). Thus, a consensus protocol is needed to add new blocks securely. It should be able to verify the correctness of the newly added blocks and seek an agreement from all nodes on the validity and sequence of these new blocks. θ-protocol [45] and quantum random number generator (QRNG) have been proposed to solve such problems. QRNG guarantees the true random selection of a verifier node. True randomness assures fairness and thus should be agreed upon among nodes. The selected verifier node is then responsible for performing a verification test of the new block and adding it to the chain. θ-protocol is then executed to "broadcast" the new block to other parties. In other words, nodes in the blockchain agree on the true randomness instead of solving a cryptographic puzzle or staking coins (e.g., proof-of-work and proof-of-stake). This is similar to leader-based consensus protocols [57]. The fundamental probabilistic property of quantum mechanics gives QRNG the ability to create true randomness, which can be clearly modelized and controlled for perpetual unpredictable randomness, contrary to the predictable randomness generated by classical deterministic processes, such as pseudorandom number generators.

Note that the QRNG machine today may have statistical biases due to noisy quantum hardware and is not realistic for use. We assume such bias can be tackled in the future. Nonetheless, the instantly produced randomness may not be able to guarantee simultaneous additions of new blocks. A complete scheme of consensus mechanisms for quantum blockchains is still under exploration [23], [45]. After the verifier (block producer) selection, the verifier node initiates the verification test (e.g., θ-protocol), which allows each node in the network to verify if a source is distributing a correct state, even in the presence of untrusted nodes. The verifier node finally adds the new block to its local quantum blockchain copy and broadcasts the addition. There are still many limitations to the implementation of quantum broadcasting. More details about broadcasting can be found in Section V. Based on QRNG and θ-protocol, we achieve a primitive consensus process for QBIF, which is discussed next.

IV. QUANTUM BLOCKCHAIN IDENTITY FRAMEWORK

The vision of QBIF is to achieve secure pseudonymization, which preserves privacy and prevents forgery. Users control their own identities and use them without revealing unnecessary information (self-sovereign identities). At the same time, identities are secure and genuine under a decentralized quantum setting. In this section, we introduce various aspects of the architecture of QBIF: roles, quantum identity attestations (QIAs), quantum blockchains, authentication, and consensus protocols.

A. ROLES

In this article, "identity" includes the user's unique id (e.g., username and social security number), attributes (pieces of information about the user's identity, e.g., name, age, balance, and address), and attestations (proofs of user statements about attributes, e.g., "birthyear $==$ 1999" and "income $>$ 50 000"). We also use "public credential" to refer to a user's public identity information (unique id and attestations). Identity attributes are private to users (owners). Attribute-based identity authentication, which verifies identity attributes without revealing additional information, is a prevalent way to authenticate users with anonymity (pseudonymization) [58], [59].

Users can prove that they satisfy the conditions set by identity verifiers without revealing their actual identity information. Identity verifiers authenticate users by verifying the issuers' signatures on the attestations. For example, a bank may loan money only to users whose annual incomes exceed \$50 000. When the bank (verifier) evaluates a user's financial information for a loan request, the bank can verify the user's annual income by checking the signature on the user's attestation without looking at the user's actual income number. Keeping attestations on a blockchain ensures their authenticity. Identity attributes are private to owners. Decentralized identity removes the concerns of privacy violation and single-point-of-failure.

As in the classical approach, there are three roles in QBIF: identity owners, identity issuers, and identity verifiers. Identity issuers represent trusted parties, such as local governments or big companies. Issuers issue identities, such as personal IDs or user profiles in an application/software. They also attest (not issue) the validity of identity attributes and issue attestations. For example, a bank only issues attestations about users' financial information. An attestation process is started on the user's demand and finished by an issuer. The reliability of an attestation depends on the reputation of the issuer. Only attestations are stored on blockchains. Ownership is marked by double signatures, as discussed in subsection E.

Users keep their identities at discretion (preferably privately) and use only the on-chain attestations to prove statements about their identity attributes to verifiers. The verifiers provide services according to the reputation of the issuers who attested the identity statements.

In QBIF, attestations are kept in the form of quantum states and are chained together by entanglement. These are called QIAs. Issuers do the generation of QIA. Verifiers on user's demand do authentication of QIA. Identity owners (users), who want authorized actions from verifiers, must go through authentication and attestation processes if they have not done that with the issuers.

B. QUANTUM IDENTITY ATTESTATIONS (QIAS)

Attestations are evidence about users' identity statements. They could be in any form (e.g., hash values, encrypted messages, or bit strings). Here, we assume to keep them in bit strings for simplicity. QIAs in QBIF are quantum states containing such bit strings, which could be created by converting them into qubits [60], [61]. Nonetheless, one user can have multiple QIAs (for different identity attributes). Let ψ be the bit string of attestation that consists of n bits; then, a QIA can be represented as

$$L_\varphi|0^{\otimes n}\rangle = |\psi\rangle = |\, b_1 b_2 \cdots b_n\rangle. \tag{11}$$

A QIA should be double-signed (by the owner and the issuer) before use, and a signed QIA can be represented as $|\psi\rangle'$ as indicated in (12). Signatures are interactively done between an owner and an issuer (signed with private keys from both parties) as discussed in Section III-C. $|\psi\rangle'$ has $n + 2(n + m)$ qubits after double-sign, where n is the length of ψ and m is the output length of h defined in (4)

$$|\psi\rangle' = |\psi\rangle \,|\, h^u\left(\psi, \rho_1^u\right)\rangle \,|h^i\left(\psi, h^u\left(\psi, \rho_1^u\right), \rho_1^i\right)\rangle. \tag{12}$$

The superscripts indicate which party (u: user and i: issuer) h or ρ_1 belongs to. A QIA is prepared by an issuer per user request in the attestation process. QIAs are double-signed (as $|\psi\rangle'$) and are kept in the chain of quantum states. Signing with the issuer's private key indicates that the issuer agrees with the user's attested statement. Signing with the user's private key demonstrates the ownership of the attestation. No trusted centralized storage is needed.

C. QIAS ON QUANTUM BLOCKCHAIN

We assume a quantum network and achieve decentralization over quantum blockchains. QBIF provides distributed identity management and a primitive consensus protocol for coordinating network nodes (consisting of users, issuers, and verifiers). Nodes are interconnected by quantum communication channels. As shown in Fig. 3, each party keeps a copy of the chain of quantum states that holds the signed QIAs chronologically. The list of signed QIAs is kept on the chain in the form shown in (10).

Issuers and verifiers are candidates for block producers (e.g., miners on proof-of-work blockchains). The owner of a QIA and the issuer must double-sign the QIA before

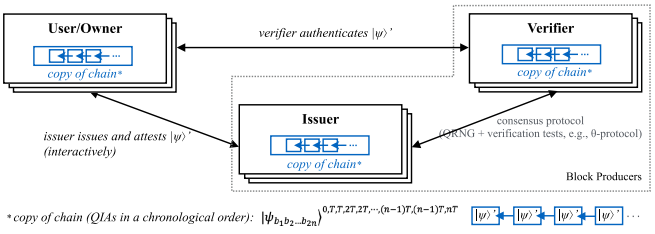


FIGURE 3. Roles and interactions on QBIF.

it goes into the block pool, i.e., candidate blocks to be attached to the chain. Block producers add these blocks to the chain after a consensus process (Section IV-D). The ownership of the signed QIA is demonstrated by the owner's signature, and the validity of the QIA is marked by the issuer's signature. As discussed, the signature could only be done by an interactive signature process. Any QIA signed without the consent of both parties is invalid and does not pass the consensus process.

Once a QIA is put on the chain, the owner can initiate an action with a verifier by sending the location of the signed QIA on the blockchain. The verifier determines the authenticity of the QIA by validating the signed QIA with the user's and the issuer's public keys. No additional knowledge of personal identity is needed during the authentication.

Note that the level of validity for an attestation can be defined by an issuer so that a user can meet whatever level a verifier may require. The level of validity can be determined by way of issuance or attestation, such as verifying in person, with biometric readers, via password, online, etc. The level of validity can be integrated into QIAs by adding extra qubits describing the level.

Since we are dealing with a primitive quantum blockchain structure, there are no sophisticated event triggers such as those used in smart contracts in classical blockchain-based applications. Thus, part of the communication would be off-chain, such as the online verification mentioned above. A hybrid network of classical and quantum communications would be the most plausible transition from classical internet to quantum internet as quantum technology develops. QKD is one good example.

In QBIF, quantum PKI and quantum blockchain processes are executed on quantum communication channels. Other interactions, such as off-chain attestations and agreements, are kept on classical channels. As shown in Fig. 4, the network of QBIF is composed of multiple quantum nodes connected via a quantum network in a peer-to-peer fashion. The classical channels are neglected in the figure but coexist with the quantum channels. Each node is a quantum system hosting a copy of the quantum blockchain, combined with a classical system dealing with off-chain communications.

D. CONSENSUS PROTOCOL

As discussed earlier, consensus protocols of a quantum blockchain are primitive due to the difficulty of implementing block producers' election (or competition). The most

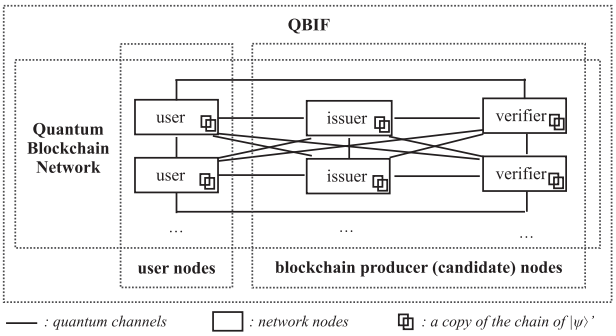


FIGURE 4. QBIF network.

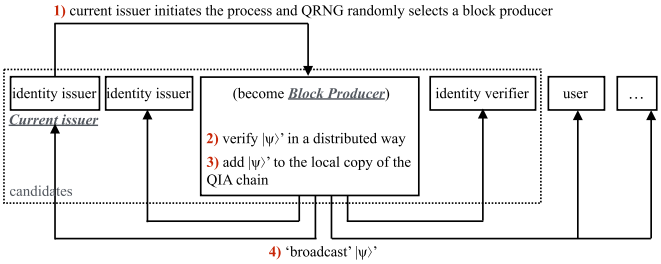


FIGURE 5. Consensus process.

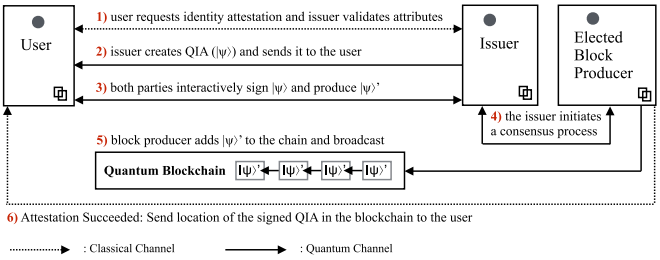


FIGURE 6. Attestation process.

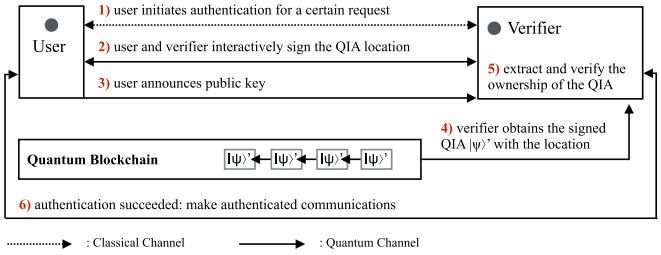


FIGURE 7. Authentication process.

prevalent consensus protocols for classical blockchains are proof-of-work (mining) in Bitcoin or proof-of-stake (voting) in Ethereum. Here, we propose to use QRNG and distributed verification tests (e.g., θ-protocol) to emulate an initial consensus protocol for quantum blockchains. QRNG guarantees true randomness in selecting a block producer (who is also responsible for validating a new block). Here, the true randomness of QRNG replaces the fair competition/election provided by proof-of-work or proof-of-stake. The selected block producer then executes a distributed verification test to validate the newly added GHZ state (the new block). The distributed verification process keeps the quantum system validated even with untrusted network nodes [45]. Once the verification tests are done, the new block is added to the blockchain. Then, the new chain is broadcasted to all network nodes. Together with Fig. 5, the following steps describe the consensus process of QBIF.

1) By now, a double-signed QIA ($|\psi\rangle'$) has been created by an issuer and a user. $|\psi\rangle'$ is waiting to be added to the blockchain. The issuer of $|\psi\rangle'$ initiates the consensus process and activates a QRNG to randomly select a blockchain producer among the candidates.
2) A candidate is selected by the QRNG. If the candidate is unavailable, the QRNG is executed again until an available candidate is selected. We assume the selected candidate is trustworthy (i.e., candidates are trusted). Suppose the third node in Fig. 5 is available and is selected. It then takes the role of block producer and initiates the distributed verification. For example, in [45], a pass condition and a set of random angles $\theta_j \in [0, \pi)$ are defined in advance, $j \in \{12, \ldots, n\}$. θ_j represents the measurement basis of node j, and the verification runs until all the network nodes satisfy the pass condition. For an ideal GHZ state, the verification will succeed theoretically with 100% probability. However, this probability is varied according to entanglement fidelity. $|\psi\rangle'$ is accepted only when the majority of nodes pass the condition [45].
3) Once we have a valid $|\psi\rangle'$, the block producer then fuses $|\psi\rangle'$ into a four-photon GHZ state with the latest on-chain state (10), which adds $|\psi\rangle'$ to its local copy of the QIA chain.
4) Then, the block producer "broadcasts" $|\psi\rangle'$ to all network nodes. Note that the verification protocol in [45] involves more than merely implementing verification tests. It also links the outcome of the verification tests, the validated state, to the target state. In other words, the newly added block has also been copied and distributed to all other network nodes during the verification tests. This distribution of the new block remedies the broadcasting limitations of quantum networks. This is discussed further in Section V.

E. ATTESTATION AND AUTHENTICATION

Identity attestation and authentication are two critical processes of QBIF. The attestation process produces QIAs, and the authentication process uses QIAs. In Figs. 6 and 7, dashed arrow lines refer to classical communication channels, and solid arrow lines represent quantum channels.

Attestation process: The attestation process is completed by collaboration between the user and an issuer. This process creates QIAs and makes interactive signatures. Fig. 6 shows a step-by-step attestation process. Together with Fig. 6, the following steps describe the identity attestation process.

1) A user initiates the process by requesting an identity attestation. The user defines the statements about the identity attributes (e.g., income $>$ 50 000). The issuer validates the user's identity attributes. This step can be done over a classical communication channel.
2) The issuer prepares the QIA $|\psi\rangle$ (11) and sends it to the user over a quantum communication channel.
3) The user receives $|\psi\rangle$ and starts the interactive signature (as discussed in Section III-C) with the issuer. $|\psi\rangle$ is first interactively signed with the user's private key and then with the issuer's private key (12). The interactive signatures prove the ownership and the validity of the QIA. After $|\psi\rangle$ is signed from both sides, $|\psi\rangle'$ is ready.
4) The issuer initiates the consensus process by activating the QRNG.
5) The selected block producer starts the distributed verification tests. If the tests are passed, $|\psi\rangle'$ is added to the QIA chain and is broadcasted to the network.
6) The block producer sends the location nT of $|\psi\rangle'$ in the blockchain to the user using a classical communication channel. Since there is no available DID to identify users in QBIF (which is generally used by blockchain-based identity), the user keeps the signed QIA's location. It is shown to the verifier in the authentication process and used to localize the user's signed QIA. The user can claim ownership of this signed QIA by private key.

Authentication process: The authentication process happens between a user and a verifier when the user requests an authorized action. It requires a signed on-chain QIA corresponding to the action's requirements. The verifier extracts the signed QIA and uses it to authenticate the user. As shown in Fig. 7, the following steps describe the authentication process.

1) A user requests an authorized action provided by a verifier, which initiates the authentication process. The verifier verifies whether the user satisfies the requirement (e.g., if the user's annual income exceeds \$50 000 when applying for a loan).
2) The user interactively signs the QIA location nT (as $|nT\rangle\ |f(nT, \rho_1^{u\_l})\rangle$) with the verifier using the same private key as the one used for signing the QIA and then sends it to the verifier. This signature of location nT proves the user's ownership of the private key used to sign the QIA. As discussed in Section III-C, only an interactive signature process can guarantee a signature's validity (not someone pretending to own this signature). Therefore, the user must interactively sign and send the QIA location to the verifier through a quantum channel.
3) The user announces his/her public key if necessary.
4) The verifier extracts the identity location nT according to (6). By nT, the verifier finds and obtains the signed QIA $|\psi\rangle'$.

Algorithm 1: Extract and Verify a QIA.

Quantum transformation: U^{evqia}
Input: $|\psi\rangle^{'}, |nT\rangle\ |f(nT, \rho_1^{u\_l})\rangle\ ,\ h, \rho_1^u\ , \rho_2^u,\ \ \rho_1^{u\_l},\ \ \rho_2^{u\_l}$

```
#Superscript denotation: (u: user, i: issuer, u_l: QIA location).

#Extract |ψ⟩′ by the issuer's public key
|ψ⟩′ = |ψ⟩ |h^u(ψ, ρ_1^u)⟩ |h^i(ψ, h^u(ψ, ρ_1^u), ρ_1^i)⟩
→ |ψ⟩|h^u(ψ, ρ_1^u)⟩ |0⟩

#Extract |ψ⟩ |h^u(ψ, ρ_1^u)⟩ |0⟩ by the user's public key
(ρ_r^{u'}, ρ_s^{u'}) = h(ρ_1^u, ρ_2^u)
if ρ_r^u ==
ρ_r^{u'} && M(|ψ⟩ |h^u(ψ, ρ_1^u)⟩ |0⟩, index_last) is |0⟩
then

  #Extract |nT⟩ |f(nT, ρ_1^{u_l})⟩ by the user's public key and verify signatures
  |nT⟩ |f(nT, ρ_1^{u_l})⟩ →|nT⟩ |0⟩
  (ρ_r^{u_l'}, ρ_s^{u'}) = h(ρ_1^{u_l}, ρ_2^{u_l})
  if ρ_r^{u_l} ==
  ρ_r^{u_l'} && M(|nT⟩ |0⟩, index_last) is |0⟩ && ρ_1^{u_l} == ρ_1^u
  then

    |ψ⟩ |h^u(ψ, ρ_1^u)⟩ |0⟩ → |ψ⟩ |h^u(ψ, ρ_1^u)⟩ →
    |ψ⟩ |0⟩ → |ψ⟩
    return |ψ⟩ #Succeed

  end if

end if
```

5) The verifier verifies the signatures of $|\psi\rangle'$ with the issuer and the user's public key. If the signature is valid, the verifier uses ψ to determine the authentication result. Based on (6) and (12), the extraction and verification of $|\psi\rangle'$ is described in Algorithm 1.
6) If the process succeeds, the verifier makes authenticated communications with the user (Section III-C) and proceeds with the requested service. (e.g., the verifier successfully verifies that the user's income exceeds \$50 000 and proceeds with the subsequent loan application procedures.)

F. SYSTEM SECURITY

The security of QBIF is mainly based on the quantum trapdoor one-way functions (2) and the secure nature of quantum physics (unconditional security). Here, we discuss the security aspects of QBIF:

Quantum-proof: As discussed, classical blockchains' security is vulnerable to quantum computing. Quantum

IEEE Transactions on Quantum Engineering

blockchains are immune to any notable quantum and classical attack.

Data integrity: Classical blockchains use hash functions to chain blocks (and Merkle trees to organize transactions) and thus are sensitive to data tampering. If a random on-chain block is tampered with, all its following blocks become invalid because each block points to its previous block. The link of hash values is broken from the tampered block to the latest block. For quantum blockchains, such sensitivity has been kept and amplified by entanglement. One change to a single block could demolish the whole copy of the state chain [13], [24].

Anti-spoofing: Assume that an attacker wants to perform a spoofing attack, masquerading as a user to claim the user's on-chain attestations. The attacker's goal is to pass an authentication process fraudulently. Suppose the attacker has infiltrated the quantum channel between the user and the verifier (steps 2 and 3 in Fig. 7). The attacker can now intercept the communication of the QIA location. However, the attacker still needs to interactively sign it with the verifier. If the attacker uses his/her own private key and sends his/her public key, the verifier is not able to extract the signed QIA by this public key and ρ_1 [(5) and (6)]. ρ_1^{attacker} of the signed QIA location is not the same as ρ_1^{user} of the signed QIA.

Privacy: On-chain attestations are proofs of statements about users' identity attributes without actual identity information (pseudonymization). Such granular statements would not reveal much information, even if leaked. Pseudonymization protects privacy through the noncorrelation principles [58].

V. CHALLENGES AND LIMITATIONS

Quantum blockchains are naturally immune to quantum attacks on classical algorithms. It is exciting to see the possibility of layering blockchains on a quantum system, even though it is not pure quantum (but a hybrid with classical systems). In the QBIF conceptual design, every preliminary technology has been explicitly shown to be experimentally realizable, even though some are only in their simplest form. The proposed conceptual design does not yet meet immediate deployment requirements, but it shows a visible path toward realizing a decentralized quantum application. Nonetheless, many challenges and limitations of quantum approaches are inevitable at this stage. We discuss the main challenges and limitations of QBIF next.

A. LACK OF IMPLEMENTATION

QBIF and most quantum blockchains lack low-level specifics, which would contribute to the detailed implementation of their essential components. Implementations of many quantum technologies are still varying and require much further experimentation. Quantum blockchains are still in their very early phase. Quantum systems are mostly implemented in simulators or quantum computers with limited resources. It would not add much value to the work at this stage by introducing implementation details.

B. LIMITED QUANTUM HARDWARE

The development of quantum computers has been rapid in recent years. However, it still needs a significant time before it can support large or medium-scale computation (and connection). Current quantum computers are extremely sensitive to interactions; thus, their computation results usually have much noise. Besides, quantum states tend to gradually disintegrate due to quantum decoherence, which demands quantum error correction [62]. State discrimination strategies must be applied to fine-tune the tradeoffs between error rate and information gain [63]. In terms of authentication, the validation of a whole process would be determined or significantly influenced by the quantum bit error rate [22], [41].

C. BROADCAST LIMITATIONS

The ability to distribute entangled states to network nodes is significant for a decentralized quantum network. Theoretical analyses on point-to-point quantum communication have constantly been progressing. Quantum repeaters make possible long-distance quantum communications over bipartite quantum channels. However, point-to-point communication is not enough for a sophisticated network. A quantum broadcast network would be able to distribute entangled qubits efficiently. Current quantum broadcast networks are usually accomplished with the assistance of classical communications [64]. The upper and lower bounds of quantum broadcast networks are still limited [65], and a complex network typically introduces more noise and losses.

D. TEMPORAL ENTANGLEMENT

There are still many open problems with quantum entanglement in time [13], [66], [67]. Entanglement in time is based on entangled history theory, which is a substantial modification of the decoherent history theory (or consistent history theory). Entanglement in time shares similar properties with the general entanglement in space [54], but temporal quantum effects might be highly unstable as time passes.

E. DIFFICULTY IN ACCESSING STATES

Previous blocks on quantum blockchains based on entanglement in time are physically no longer existent. Blocks do not simultaneously coexist. It is only natural to retrieve the latest block. Previous on-chain states are hard to access. However, it is possible to transfer the past quantum correlation between quantum states so that past states can be obtained, even if they do not coexist simultaneously [50]. Moreover, quantum logic is inherently reversible; thus, propagating back in time to a previous block will unentangle qubits and potentially destroy the chain. Fortunately, through the consensus process, we have many copies of the chain on the blockchain nodes. Hence, the system is feasible as long as the majority of the blockchain nodes still keep the copies. How to make the system more sustainable than this remains future work.

F. OVERHEAD

Network overhead is significantly increased since signatures are done interactively between two parties. Signature processes are common in blockchains. Moreover, many quantum signatures can only be validated once. This would significantly increase the number of signature processes and potentially overload the network nodes. Quantum fingerprints could replace such interactive signatures to void this issue.

G. SCALABILITY

Scalability is always an issue in quantum applications due to the current scale of quantum computers and networks. In terms of quantum blockchains, one transaction per block is clearly deficient. A complex quantum data structure must be developed before a quantum blockchain can become comparable to its classical counterpart.

H. PRIMITIVE CONSENSUS

The current consensus protocol is still primitive, lacking perfect competition/election rules to create blocks. QRNG is temporarily used as a basic consensus protocol. However, QRNG cannot guarantee the normal operation of simultaneous communications in a decentralized network.

I. LOW EFFICIENCY

Performance issues of quantum blockchains exist in the information preparation [61], [68], block size [13], and cost-effectiveness strategies between the used qubit and the created block [55]. Blockchain size is a challenge for classical blockchains also due to data explosion.

J. SEMI-DECENTRALIZATION

The classical identity management and this approach require third-party authorities to verify user attestations and thus are not actual decentralization but semi-decentralization. The idea is similar to what a consortium blockchain provides, in which each member is a group of nodes who believe in the same authorities [69]. A semi-decentralization could lead to the dictatorship of resources by a small group of powerful entities. However, we believe a proper combination of decentralization and centralization is beneficial since there are always harmful contents that could inundate the network without censorship. How an ultimate decentralization can be achieved in the quantum domain (or in any future form of the internet) remains future work.

VI. CONCLUSION

Quantum computers threaten classical blockchains' security, and thus quantum blockchains are needed. This article theoretically analyzes the quantum blockchain technologies that could be used for a decentralized purpose. We review the technical evidence and put together a conceptual design for decentralized quantum identity, which is named QBIF. We investigate the essential components and the feasibility, effectiveness, and limitations of QBIF. We complete the design of QBIF by integrating existing quantum approaches, such as quantum PKIs and quantum blockchains. Nonetheless, the conceptual design still has technical gaps in detailed low-level specifics. Despite the limitations and challenges, we believe a decentralized perspective of quantum applications is noteworthy and likely.

REFERENCES

[1] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surv. Tut.*, vol. 21, no. 1, pp. 858–880, Jan.–Mar. 2019, doi: 10.1109/COMST.2018.2863956.

[2] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183–187, 2017, doi: 10.1007/s12599-017-0467-3.

[3] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 107, pp. 841–853, 2020, doi: 10.1016/j.future.2017.08.020.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Accessed: Jun. 14, 2022. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[5] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.

[6] L. K. Grover, "A fast quantum mechanical algorithm for database search," 1996, *arXiv:quant-ph/9605043*, doi: 10.48550/arXiv.quant-ph/9605043.

[7] A. Hosoyamada and Y. Sasaki, "Quantum collision attacks on reduced SHA-256 and SHA-512," in *Proc. Annu. Int. Cryptol. Conf.*, 2021, pp. 616–646, doi: 10.1007/978-3-030-84242-0_22.

[8] S. S. Tannu and M. K. Qureshi, "Not all qubits are created equal: A case for variability-aware policies for NISQ-Era quantum computers," in *Proc. 24th Int. Conf. Architectural Support Program. Lang. Oper. Syst.*, 2019, pp. 987–999, doi: 10.1145/3297858.3304007.

[9] B. Rodenburg and S. P. Pappas, "Blockchain and quantum computing," MITRE Corp., Bedford, MA, USA, Tech. Rep., 2017. Accessed: Jun. 14. 2022. [Online]. Available: https://apps.dtic.mil/sti/citations/AD1125436

[10] J. J. Kearney and C. A. Perez-Delgado, "Vulnerability of blockchain technologies to quantum attacks," *Array*, vol. 10, 2021, Art. no. 100065, doi: 10.1016/j.array.2021.100065.

[11] D. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, pp. 188–194, 2017, doi: 10.1038/nature23461.

[12] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020, doi: 10.1109/ACCESS.2020.2968985.

[13] D. Rajan and M. Visser, "Quantum blockchain using entanglement in time," *Quantum Rep.*, vol. 1, no. 1, pp. 3–11, 2019, doi: 10.3390/quantum1010002.

[14] C. Simon, "Towards a global quantum network," *Nature Photon.*, vol. 11, pp. 678–680, 2017, doi: 10.1038/s41566-017-0032-0.

[15] M. Edwards, A. Mashatan, and S. Ghose, "A review of quantum and hybrid quantum/classical blockchain protocols," *Quantum Inf. Process.*, vol. 19, 2020, Art. no. 184, doi: 10.1007/s11128-020-02672-y.

[16] E. O. Kiktenko et al., "Quantum-secured blockchain," *Quantum Sci. Technol.*, vol. 3, no. 3, 2018, Art. no. 035004, doi: 10.1088/2058-9565/aabc6b.

[17] X. Sun, Q. Wang, P. Kulicki, and X. Zhao, "Quantum-enhanced logic-based blockchain I: Quantum honest-success Byzantine agreement and qulogicoin," 2018, *arXiv:1805.06768*, doi: 10.48550/arXiv.1805.06768.

[18] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K. R. Choo, "Blockchain-based identity management systems: A review," *J. Netw. Comput. Appl.*, vol. 166, 2020, Art. no. 102731, doi: 10.1016/j.jnca.2020.102731.

[19] "Ethereum whitepaper," Ethereum.org, Accessed: Jun. 14. 2014. [Online]. Available: https://ethereum.org/en/whitepaper/

[20] Y. Gao, X. Chen, Y. Chen, Y. Sun, X. Niu, and Y. Yang, "A secure cryptocurrency scheme based on post-quantum blockchain," *IEEE Access*, vol. 6, pp. 27205–27213, 2018, doi: 10.1109/ACCESS.2018.2827203.

[21] F. M. Ablayev, D. A. Bulychkov, D. A. Sapaev, A. V. Vasiliev, and M. T. Ziatdinov, "Quantum-assisted blockchain," *Lobachevskii J. Math.*, vol. 39, pp. 957–960, 2018, doi: 10.1134/S1995080218070028.

[22] X. Zhang, "One-way quantum identity authentication based on public key," *Chin. Sci. Bull.*, vol. 54, pp. 2018–2021, 2009, doi: 10.1007/s11434-009-0350-9.

[23] X. Sun, M. Sopek, Q. Wang, and P. Kulicki, "Towards quantum-secured permissioned blockchain: Signature, consensus, and logic," *Entropy*, vol. 21, no. 9, 2019, Art. no. 887, doi: 10.3390/e21090887.

[24] D. Shrier, W. Wu, and A. Pentland, "Blockchain & infrastructure (identity, data security)," *MIT-Connection Sci.*, vol. 1, no. 3, pp. 1–19, 2016. [Online]. Available: https://www.getsmarter.com/blog/wp-content/uploads/2017/07/mit_blockchain_and_infrastructure_report.pdf

[25] O. Jacobovitz, "Blockchain for identity management," Ben-Gurion Univ., Beer Sheva, Israel, 2016, Accessed: Jun. 14. 2022. [Online]. Available: https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf

[26] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Trans. Eng. Manage.*, vol. 67, no. 4, pp. 1008–1027, Nov. 2020, doi: 10.1109/TEM.2019.2926471.

[27] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Secur. Privacy*, vol. 16, no. 4, pp. 20–29, Jul./Aug. 2018, doi: 10.1109/MSP.2018.3111247.

[28] "Enter pangea, the internet of sovereignty," Bitnation, Accessed: Jun. 14. 2022. [Online]. Available: https://tse.bitnation.co/

[29] "Unlock web3, build on ethereum, collaborate worldwide," ConsenSys, Accessed: Jun. 14. 2022. [Online]. Available: https://consensys.net/

[30] "Welcome to the new internet for decentralized apps," OneName, Accessed: Jun. 14. 2022. [Online]. Available: https://onename.com/

[31] "It's your identity. own it," ShoCard, Accessed: Jun. 14. 2022. [Online]. Available: http://shocard.com/

[32] "Your login box. Powered by the blockchain," Tykn, Accessed: Jun. 14. 2022. [Online]. Available: https://tykn.tech/

[33] X. Zhu and Y. Badr, "A survey on blockchain-based identity management systems for the internet of things," in *Proc. IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Social Comput. IEEE Smart Data*, 2018, pp. 1568–1573, doi: 10.1109/Cybermatics_2018.2018.00263.

[34] Z. Gao et al., "Blockchain-based identity management with mobile device," in *Proc. 1st Workshop Cryptocurrency Blockchain Distrib. Syst.*, 2018, pp. 66–70, doi: 10.1145/3211933.3211945.

[35] G. Iovane, "Computational quantum key distribution (CQKD) on decentralized ledger and blockchain," *J. Discrete Math. Sci. Cryptogr.*, vol. 24, no. 4, pp. 1021–1042, 2021, doi: 10.1080/09720529.2020.1820691.

[36] K. Ikeda, "qBitcoin: A peer-to-peer quantum cash system," in *Proc. Sci. Inf. Conf.*, 2018, pp. 763–771, doi: 10.1007/978-3-030-01174-1_58.

[37] Y. Gao, X. Chen, G. Xu, K. Yuan, W. Liu, and Y. Yang, "A novel quantum blockchain scheme base on quantum entanglement and DPoS," *Quantum Inf. Process.*, vol. 19, no. 12, 2020, Art. no. 420, doi: 10.1007/s11128-020-02915-y.

[38] L. Gyongyosi and S. Imre, "Decentralized base-graph routing for the quantum internet," *Phys. Rev. A*, vol. 98, no. 2, 2018, Art. no. 022310, doi: 10.1103/PhysRevA.98.022310.

[39] C. Li, Y. Xu, J. Tang, and W. Liu, "Quantum blockchain: A decentralized, encrypted and distributed database based on quantum mechanics," *J. Quantum Comput.*, vol. 1, no. 2, 2019, Art. no. 49, doi: 10.32604/jqc.2019.06715.

[40] H. Buhrman, R. Cleve, J. Watrous, and R. Wolf, "Quantum fingerprinting," *Phys. Rev. Lett.*, vol. 87, 2001, Art. no. 167902, doi: 10.1103/PhysRevLett.87.167902.

[41] C. Hong, J. Heo, J. G. Jang, and D. Kwon, "Quantum identity authentication with single photon," *Quantum Inf. Process.*, vol. 16, 2017, Art. no. 236, doi: 10.1007/s11128-017-1681-0.

[42] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proc. Roy. Soc. A: Math. Phys. Eng. Sci.*, vol. 439, no. 1907, pp. 553–558, 1992, doi: 10.1098/rspa.1992.0167.

[43] R. Valivarthi et al., "Teleportation systems toward a quantum internet," *PRX Quantum*, vol. 1, no. 2, 2020, Art. no. 020317, doi: 10.1103/PRXQuantum.1.020317.

[44] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and W. K. Wootters, "Remote state preparation," *Phys. Rev. Lett.*, vol. 87, 2001, Art. no. 077902, doi: 10.1103/PhysRevLett.87.077902.

[45] W. McCutcheon et al., "Experimental verification of multipartite entanglement in quantum networks," *Nature Commun.*, vol. 7, 2016, Art. no. 13251, doi: 10.1038/ncomms13251.

[46] A. Kawachi and C. Portmann, "On the power of quantum encryption keys," in *Proc. Int. Workshop Post-Quantum Cryptogr.*, 2008, pp. 165–180, doi: 10.1007/978-3-540-88403-3_12.

[47] A. Ambainis, M. Mosca, A. Tapp, and R. De Wolf, "Private quantum channels," in *Proc. 41st Annu. Symp. Found. Comput. Sci.*, 2000, pp. 547–553, doi: 10.1109/SFCS.2000.892142.

[48] M. Liang and L. Yang, "Public-key encryption and authentication of quantum information," *Sci. China Phys. Mech. Astron.*, vol. 55, pp. 1618–1629, 2012, doi: 10.1007/s11433-011-4806-y.

[49] L. Yang, M. Liang, B. Li, L. Hu, and D. Feng, "Quantum public-key cryptosystems based on induced trapdoor one-way transformations," 2010, *arXiv:1012.5249*, doi: 10.48550/arXiv.1012.5249.

[50] C. Sabín, B. Peropadre, M. del Rey, and E. Martín-Martínez, "Extracting past-future vacuum correlations using circuit QED," *Phys. Rev. Lett.*, vol. 109, 2012, Art. no. 033602, doi: 10.1103/PhysRevLett.109.033602.

[51] D. Greenberger, M. A. Horne, and A. Zeilinger, "Going beyond bell's theorem," in *Bell's Theorem, Quantum Theory and Concept. of the Universe* (Fundamental Theories of Physics), vol. 37. Dordrecht, The Netherlands: Springer, 1989, doi: 10.1007/978-94-017-0849-4_10.

[52] G. Carvacho, F. Graffitti, V. D'Ambrosio, B. C. Hiesmayr, and F. Sciarrino, "Experimental investigation on the geometry of GHZ states," *Sci. Rep.*, vol. 7, 2017, Art. no. 13265, doi: 10.1038/s41598-017-13124-6.

[53] E. Megidish, A. Halevy, T. Shacham, T. Dvir, L. Dovrat, and H. S. Eisenberg, "Entanglement between photons that have never coexisted," *Phys. Rev. Lett.*, vol. 110, 2013, Art. no. 210403, doi: 10.1103/PhysRevLett.110.210403.

[54] D. E. Bruschi, C. Sabín, A. White, V. Baccetti, D. K. L. Oi, and I. Fuentes, "Testing the effects of gravity and motion on quantum entanglement in space-based experiments," *New J. Phys.*, vol. 16, 2014, Art. no. 053041, doi: 10.1088/1367-2630/16/5/053041.

[55] S. Banerjee, A. Mukherjee, and P. K. Panigrahi, "Quantum blockchain using weighted hypergraph states," *Phys. Rev. Res.*, vol. 2, 2020, Art. no. 013322, doi: 10.1103/PhysRevResearch.2.013322.

[56] A. J. Bennet and S. Daryanoosh, "Energy-efficient mining on a quantum-enabled blockchain using light," *Ledger*, vol. 4, pp. 82–107, Jul. 2019, doi: 10.5195/ledger.2019.143.

[57] A. Mostefaoui and M. Raynal, "Leader-based consensus," *Parallel Process. Lett.*, vol. 11, no. 1, pp. 95–107, 2001, doi: 10.1142/S0129626401000452.

[58] K. Pinter, D. Schmelz, R. Lamber, S. Strobl, and T. Grechenig, "Towards a Multi-party, blockchain-based identity verification solution to implement clear name laws for online media platforms," in *Business Process Management: Blockchain and Central and Eastern Europe Forum* (Lecture Notes in Business Information Processing), vol. 361. Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-030-30429-4_11.

[59] M. Al-Bassam, "SCPKI: A smart contract-based PKI and identity system," in *Proc. ACM Workshop Blockchain, Cryptocurrency Contracts*, 2017, pp. 35–40, doi: 10.1145/3055518.3055530.

[60] Y. Wang and Y. Zhan, "A theoretical scheme for zero-knowledge proof quantum identity authentication," *Acta Physica Sinica*, vol. 58, no. 11, pp. 7668–7671, 2009, doi: 10.7498/aps.58.7668.

[61] J. A. Cortese and T. M. Braje, "Loading classical data into a quantum computer," 2018, *arXiv:1803.01958*, doi: 10.48550/arXiv.1803.01958.

[62] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, no. 2, pp. 1098–1106, 1996, doi: 10.1103/PhysRevA.54.1098.

[63] S. S. Tannu and M. K. Qureshi, "Not all qubits are created equal: A case for variability-aware policies for NISQ-Era quantum computers," in *Proc. 24th Int. Conf. Architectural Support Program. Lang. Oper. Syst.*, 2019, pp. 987–999, doi: 10.1145/3297858.3304007.

[64] J. Yard, P. Hayden, and I. Devetak, "Quantum broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 7147–7162, Oct. 2011, doi: 10.1109/TIT.2011.2165811.

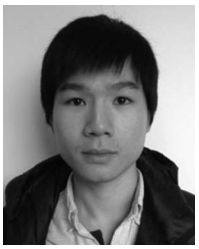
[65] S. Bäuml and K. Azuma, "Fundamental limitation on quantum broadcast networks," *Quantum Sci. Technol.*, vol. 2, 2017, Art. no. 024004, doi: 10.1088/2058-9565/aa6d3c.

[66] M. Nowakowski, "Quantum entanglement in time," in *Proc. AIP Conf. Proc.*, 2017, Art. no. 020007, doi: 10.1063/1.4982771.

[67] D. Rajan, "Quantum entanglement in time," 2020, *arXiv:2007.05969*, doi: 10.48550/arXiv.2007.05969.

[68] K. Mitarai, M. Kitagawa, and K. Fujii, "Quantum analog-digital conversion," *Phys. Rev. A*, vol. 99, 2019, Art. no. 012301, doi: 10.1103/PhysRevA.99.012301.

[69] O. Dib, K. L. Brousmiche, A. Durand, E. Thea, and E. B. Hamida, "Consortium blockchains: Overview, applications and challenges," *Int. J. Adv. Telecommun.*, vol. 11, no. 1&2, pp. 51–64, 2018. [Online]. Available: https://hal.archives-ouvertes.fr/hal-02271063



Zebo Yang (Graduate Student Member, IEEE) received the B.S. degree in computer engineering from the Guangdong University of Foreign Studies, Guangzhou, China, in 2012, and the M.S. degree in computer engineering from the Waseda University, Tokyo, Japan, in 2019. He is currently working toward the Ph.D. degree in computer engineering with the Washington University in St. Louis, St. Louis, MO, USA.

From 2011 to 2017, he worked as a Software Engineer with the Tencent, Inc., Baidu, Inc., and DJI, Inc. Since 2019, he has been working as a Graduate Research Assistant with the Washington University in St. Louis. His research interests include blockchains, quantum computing, network, and system security, machine learning, the internet of things, and wireless communications.

Tara Salman (Member, IEEE) received the B.S. degree in computer engineering and the M.S. degree in computer networking from the Qatar University, Doha, Qatar, in 2012 and 2015, respectively, and the Ph.D. degree from the Washington University, St. Louis, MO, USA, in 2021.

She is currently an Assistant Professor of computer science with the Texas Tech University, Lubbock, TX, USA. Previously, she was a Graduate Research Assistant with the Washington University in St. Louis (2015–2021) and a Research Assistant with the Qatar University (2012–2015). She has authored 1 book chapter, a patent, and more than 20 internationally recognized conferences and journals. Her research interests include blockchains, network security, distributed systems, the internet of things, and financial technology.

Raj Jain (Life Fellow, IEEE) received the B.E. degree in electrical engineering from the APS University, Rewa, India, in 1972, the M.E. degree in automation from the Indian Institute of Science, Bangalore, India, in 1974, and the Ph.D. degree in applied mathematics (computer science) from Harvard University, Cambridge, MA, USA, in 1978.

He is currently the Barbara J. and Jerome R. Cox, Jr., Professor with the Department of Computer Science and Engineering, Washington University in St Louis, St Louis, MO, USA. He was one of the cofounders with the Nayna Networks, Inc., San Jose, CA, USA, a next-generation telecommunications systems company in San Jose. He was a Senior Consulting Engineer with the Digital Equipment Corporation, Littleton, MA, USA, and then a Computer and Information Sciences Professor with the Ohio State University, Columbus, OH, USA.

Dr. Jain is a recipient of the 2018 James B. Eads Award from the St. Louis Academy of Science, the 2017 ACM SIGCOMM Life-Time Achievement Award, and the 2015 A. A. Michelson Award from the Computer Measurement Group. He ranks among the most cited authors in Computer Science. He has authored *The Art of Computer Systems Performance Analysis*, which won the 1991 Best-Advanced How-to Book, Systems award from the Computer Press Association. He is a Fellow of the ACM and AAAS.

Roberto Di Pietro (Fellow, IEEE) received the B.S. degree in computer science and the M.S. degree in informatics from the University of Pisa, Italy, in 1994 and 2003, respectively, and the Ph.D. degree in computer science from the University of Rome, Italy, in 2004.

He is currently a Full Professor in Cybersecurity with the HBKU-CSE, Doha, Qatar. Previously, he was in the capacity of the Global Head Security Research, Nokia Bell Labs, Holmdel, NJ, USA, and an Associate Professor (with tenure) of Computer Science with the University of Padova, Padova, Italy. He also served more than 10 years as a Senior Military Technical Officer. Overall, he has worked in the cybersecurity field for more than 23 years, leading technology-oriented and research-focused teams in the private sector, government, and academia (MoD, United Nations HQ, EUROJUST, IAEA, and WIPO). Besides being involved in M&A of startups—and having founded one (exited)—he has produced 230+ scientific papers and patents over the cited topics, has coauthored three books, edited one, and contributed to a few others. His research interests include security and privacy for wired and wireless distributed systems (e.g., blockchain technology, cloud, IoT, and online social networks), virtualization security, applied cryptography, computer forensics, and data science.

Prof. Pietro is an AE for ComCom, ComNet, PerCom, *Journal of Computer Security*, and other International journals. In 2011–2012, he was the recipient of the Chair of Excellence from the University Carlos III, Madrid. In 2020, he was the recipient of the Jean-Claude Laprie Award for significantly influencing the theory and practice of Dependable Computing.