Towards a Quantum-Resistant Blockchain based on QKD

Sufyan Al-Janabi[1]

[1]College of Computer Science and IT, University of Anbar, Ramadi, Iraq

***Abstract*— Blockchain (BC) as a distributed ledger technology is getting more and more recognition in modern network technologies that are moving away from centralized toward decentralized management. However, the blockchain's security is built on the computational complexity of certain mathematical problems that cannot be solved on existing "classical" computers in an acceptable time. Nevertheless, quantum computers have the capability to effortlessly solve such problems with a significant reduction in time. The current blockchain technology relies on two main computational constructions; digital signatures and cryptographic hash functions. Both of them are threatened by the quantum computers. In this work, we report on the quantum threats to "classical" blockchain technology. The main directions to produce quantum-resistant blockchain (QB) platforms are reviewed with an emphasis on approaches based on Quantum Key Distribution (QKD). Then, some notable challenges in implementing QBs are discussed. Indeed, the future research directions in this field are identified.**

***Keywords*— Classical Blockchain, Post Quantum Cryptography, Quantum Key Distribution, Quantum Blockchain, Quantum Threat.**

1. INTRODUCTION

Blockchain (BC) technology can be used to eliminate or reduce the effect of many problems that are emerging from the centralized nature of network systems. These problems include network management and scalability issues, security and privacy concerns, and devices' interoperability and data traceability. This is because BC provisions a distributed ledger with decentralized network authority. Thus, peer-to-peer entities can manage the authentication and access to transactional data records securely and in a tamper-resistant manner [1], [2].

The security and validity of BC are founded on one-way mathematical functions that can be easily implemented in one direction but they are difficult to be calculated in the reverse direction on traditional (classical) computers. However, the current development in quantum computing is posing serious threats to BC cryptographic approaches because quantum computers can achieve an exponential computational advantage. A totally capable quantum computer can definitely in seconds perform the reverse calculations that might take years on "classical" computers. Nevertheless, reaching such levels of quantum processing power may need a decade or so to achieve. The current quantum computing prototypes called Noisy Intermediate-Scale Quantum (NISQ) devices still have practical computation limits [1].

In the meantime, different quantum algorithms have been developed to run on quantum computers. For example, Shor's quantum algorithm can break some cryptographic constructions through performing numbers' factorization with exponential speedup compared to classical devices. Moreover, Gover's algorithm can search unstructured data on quantum computers with quadratic speedup. Hence, the current use of NISQ devices can achieve a quantum advantage using various quantum and/or hybrid quantum/classical algorithms. Therefore, quantum information processing-based solutions have been proposed for addressing this issue for the deployment of quantum-safe BC networks. Indeed, it is quite prudent to expect that both quantum computation and BC will be a field of active research and some interesting development is going to be witnessed in the next decade [1], [3].

Despite that a fully-capable, reliable, and scalable quantum computer has not been built yet and its realization might need about 20 years, NISQ devices are already available in some industry and university laboratories. These can be considered as small to intermediate-scale quantum computers. already exist in universities and industry laboratories often called NISQ (Noisy intermediate Scale quantum devices). Enormous efforts are performed by technology companies including Google, Microsoft, IBM, Xanadu, and D-wave for producing large-scale universal quantum computers. These efforts have resulted in some interesting technological breakthroughs recently [4].

Quantum information technology has affected the research and industry of cryptography. In particular, the technique of Quantum Key Distribution (QKD) uses quantum physics principles for establishing secure communication channels. This is done by leveraging the quantum mechanics' inherent properties, such as Heisenberg's uncertainty principle and the no-cloning theorem, to enable the secure exchange of cryptographic keys between legitimate parties. QKD does not rely on mathematical assumptions like traditional encryption. Instead, it offers unconditional security based on the principles of quantum mechanics that ensure any attempt to measure quantum states will irreversibly disturb them. This disturbance can be used by the communicating parties to detect eavesdropping [2], [5]. QKD is combined with one-time pad encryption to achieve unconditionally secure data transmission. Indeed, the quantum-resistant blockchain (QB) can benefit from other quantum constructions such as one-way quantum

DOI:http://doi.org/10.24086/cocos2024/paper.1528

functions and quantum hash functions to implement tasks like quantum signatures and quantum voting. Hence, the classical BC is updated to the QB with additional advantages of longer data encryption and time utilization [6].

For the time being, QB constructions are in their early development phase. They need more research and implementation of the infrastructure. QB functionalities like user authentication and access control have to be established before achieving real-world quantum decentralization [7]. In response, this paper aims to explore the main approaches to achieving QB. This is done at first by reviewing quantum threats to classical BC. Then, the main focus will be on using QKD to produce QBs. The remainder of this paper is organized as follows: Section 2 gives some theoretical background of QKD and BC. Next, the quantum threats to "classical" BC are introduced in Section 3. Section 4 reviews the main approaches to realize QBs. Then, using QKD to produce QB is discussed in Section 5 before the research challenges and future directions are outlined in Section 6. Finally, the paper is concluded in Section 7.

2. Theoretical Background

This section reviews the necessary theoretical background on QKD and "classical" BC without going into every detail of these technologies as such details can be found elsewhere in the literature.

2.1 QKD Overview

QKD is a cryptographic protocol that enables two parties to securely share cryptographic keys on the basis of some basic principles of quantum mechanics. Here, we briefly describe the BB84 protocol, which is a QKD protocol developed by Bennett and Brassard in 1984. The two legitimate parties (Alice and Bob) use the BB84 protocol for securely establishing a shared key by transmitting quantum bits (qubits) over a noisy quantum channel. As soon as the shared cryptographic key is established, Alice and Bob can use it for one-time pad encryption or with other traditional encryption algorithms (e.g., the AES). The steps involved in the BB84 QKD protocol can be summarized as follows [2], [8]:

Setup Initialization: Alice generates two random bit strings of length n; a binary string A and a string B that determine the bits' encoding bases.

Qubit generation: For each bit in A, a qubit is prepared by Alice in one of two possible states based on the corresponding B bit. When the B bit is 0, the qubit is prepared in the standard basis ($\{|0\rangle, |1\rangle\}$), otherwise, the qubit is prepared in the Hadamard basis ($\{|+\rangle, |-\rangle\}$).

Qubit transmission: Alice uses the quantum channel to send the prepared qubits to Bob.

Qubit measurement: After receiving the sent qubits, Bob randomly and independently chooses a measurement basis string. For each received qubit, he measures it and records the result.

Error estimation: Alice and Bob use the classical channel for publicly announcing their respective basis strings. They keep the bits where their bases match and discard the others.

Key extraction: Alice and Bob use the bits corresponding to the matching bases to form the shared secret key.

Security verification: Alice and Bob can publicly compare a subset of their keys to calculate the error rate. Based on this, they decide whether eavesdropping has occurred or not.

Key Distillation: When the measured error rate is below a certain threshold, Alice and Bob can implement error elimination and privacy amplification procedures to distill a shorter but significantly secure shared key.

2.2 Blockchain Overview

Blockchain is a computational data structure that can provide an open distributed ledger for many interesting applications including cryptocurrencies. BC technology can be used for transferring confidential information in networks composed of untrusted nodes. BC is considered as a distributed database consisting of non-erasable information records of information, where the management is done by a group of nodes rather than a single centralized authority. The security of BC is based on two main cryptographic tasks; cryptographic hash functions and digital signatures. Each block in the BC is connected with the previous block via the hash value of the previous block. Indeed, each node has a copy of the distributed ledger. Therefore, when an eavesdropper wants to compromise the BC security, he/she needs to perform many tedious and time-consuming mathematical calculations for each network node simultaneously. This has to be very expensive and requires more "classical" computational power. This constitutes the main security strength of BC technology [9], [10].

The working of BC can be outlined according to the following steps [10]:

a) Transaction creation: The sender (Alice) is assumed to request a transaction. However, before any transmission, she needs to encrypt and authenticate the transaction data. Thus, she hashes the transaction data and then signs the hashed data using her private key in order to generate the required digital signature. Other nodes can use the corresponding public key to check the authenticity of the transaction.

b) Broadcast and validation of transaction: The transaction data and the related digital signature are next broadcasted in the BC network. The nodes in the BC network validate the transaction via the use of Alice's public key to decrypt the digital signature and then compare the result with the hashed transaction data to check the transaction's integrity. Valid transactions are added to a block.

c) Broadcast and validation of block: To produce a valid block, a block with valid transactions should be broadcast to miners in the BC network. The miners use consensus protocols for block validation. After a block is validated,

DOI:http://doi.org/10.24086/cocos2024/paper.1528

the miner will broadcast the valid block in the BC network. Hence, the valid block is added to the BC. Finally, the BC network updates the ledger of each node. Thus, the request is completed.

3. Quantum Threats to the Classical Blockchain

This section considers deficiencies of the current "classical" BC technology manifested by the recent advances in developing quantum computers. As mentioned previously, BC security relies on two basic one-way cryptographic technologies, which are hash functions and digital signatures. Most BC platforms use elliptic curve cryptography or the large integer factorization problem to generate digital signatures. However, the security of these constructions is based on the assumed computational complexity of underlying mathematical problems. It is well-known now that a universal quantum computer can efficiently solve these problems, and hence the BC security would be under question. In particular, there are two important algorithms (the so-called Shor's and Grover's quantum algorithms) that threaten the cryptographic principles of BC. Therefore, they are currently considered the biggest threat to BC. Here, these two algorithms are reviewed [4], [11]:

• Shor's algorithm: This algorithm was proposed in 1994 to solve the problem of prime number factorization. It offers an exponential speedup compared to classical computers. Thus, it enables an attacker with a quantum computing facility to compromise such cryptographic problems that are quite difficult to solve using classical computers. Shor's algorithm solves the famous problems of integer factorization and discrete logarithms in polynomial time. Hence, it represents a significant threat to the security of some widely used public key infrastructure. These include the RSA algorithm, Digital Signature Algorithm (DSA), Elliptic Curve Digital Signature Algorithm (ECDSA), and Elliptic Curve Diffie-Hellman (ECDH) algorithm. Shor's algorithm can be used to find the private key of a user from its public key. Therefore, an attacker having a quantum computer can generate that user's digital signature so he/she would compromise the BC security by including an unauthorized transaction in it.

• Grover's algorithm: This is a quantum search algorithm that offers a quadratic speedup in calculating the inverse of a hash function. It enables the so-called 51% attack, where a group of malicious parties having a majority of the computing power in the BC network can monopolize the process of new blocks' mining. Thus, Grover's algorithm compromises the BC security in two ways. At first, it enables the replacement of blocks by finding hash collisions without the attacker being spotted. Secondly, it offers a speedup for a miner having a quantum computation device to mine blocks in a way significantly faster than a miner using a classical computer. Hence, it would be possible for an attacker to insert a modified block in the BC by breaking a hash function. In this way, many blocks can be inserted and it might take a mere hours for the attackers to control the entire BC network preventing their spending transactions from recording in the BC.

There are some other quantum computing attacks on BC technology in the literature. In general, it can be said that the future BC technology would be under constant quantum computing threats of speeding up the nonces' generation, faster searching for the collisions of hash functions, and breaking the security of the public key "classical" encryption [3]. Thus, quantum computing represents a serious risk for the various BC-based solutions. This issue needs to be carefully considered in long-term planning and quantum-resistant cryptographic tools need to be developed [4]. Figure 1 summarizes the most important quantum computing threats to BC.

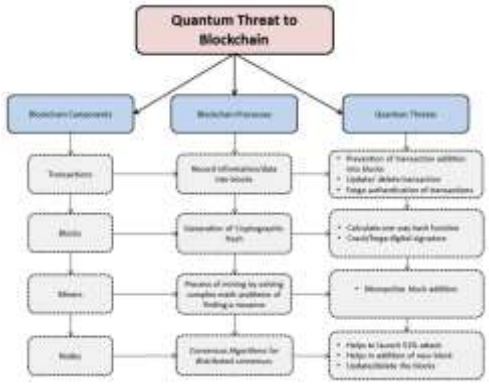

Figure 1The most important quantum computing threats to blockchain [4]

4. Quantum-Resistant Blockchain (QB)

In response to the serious threats that quantum computation imposes on BC platforms, researchers have proposed a variety of solutions that aim to increase BC security so that it can combat quantum attacks. These solutions can be grouped into two main areas of cryptography, which are quantum cryptography and post-quantum cryptography (PQC). Techniques from both of these areas are expected to produce QB infrastructures. This is discussed in the following subsections. It is important to emphasize that both quantum information itself and the defense techniques against quantum computation have not yet reached a level of high technology readiness. Thus, both subjects are witnessing active research and it is possible to see some interesting developments during the next decade.

4.1 POC-based QB

PQC involves the development of new asymmetric algorithms that can resist attacks from quantum algorithms (such as Shor's and Grover's algorithms). POC algorithms (also called quantum-resistant algorithms) do not depend upon quantum mechanical processes. They are rather based on certain mathematical problems, which are assumed to be unsolvable by neither classical nor quantum computers. This assumption must be valid at least under some reasonable circumstances. Nowadays, PQC is an expanding field. However, it still has a big deal of uncertainty as PQC algorithms do not have guaranteed security against threats. Indeed, there is a lack of worldwide standardization [4].

DOI:http://doi.org/10.24086/cocos2024/paper.1528

There is a paradigm shift from the "pre-quantum" to the "post-quantum" era. This has resulted in the development of new cryptographic primitives which are promised to be robust against quantum attacks. Those primitives are applicable in QB [12]. In particular, the BC security can be enhanced using PQC-based digital signatures for signing transactions. However, most of these digital signature schemes are computationally intensive and rely on unproven security assumptions [11].

The most promising classes of PQC systems that are believed to offer robustness against attacks from both classical and quantum computers include lattice-based cryptography, code-based cryptography, hash-based cryptography, and multivariate quadratic equations cryptography. We already have seen a variety of PQC proposals from these areas [9], [13]. However, in this paper, our concentration is mainly on the other category of quantum cryptography-based QB.

4.2 Quantum cryptography-based QB

Quantum cryptography explores the principles of quantum mechanics for performing secure cryptography tasks and detecting the existence of eavesdroppers. In this respect, the most established quantum protocol is QKD which offers guaranteed secrecy against potential eavesdropping even in the case that the eavesdropper has a quantum computer. The research in this area should lead to building quantum informational versions of BC. Other than QKD, some proposals also use quantum states for representing information, such as quantum cryptocurrencies. However, these would require developing reliable quantum state storage [9], [10].

The use of QKD for building QBs might appear to be counterintuitive. One might argue that QKD is not suitable for providing authentication because its operation requires an authenticated classical public channel. However, each QKD successful session can generate a large amount of shared secret bits. Part of these bits can be used for authenticating subsequent sessions. Thus, QKD can be used to construct digital signature functionality. In this way, QKD can be added to the current BC system for protection against quantum attacks. Nevertheless, QKD might currently be beneficial for securing small to mid-range distributed databases due to technology limitations [11].

The obvious advantage of using QKD for developing QBs compared to PQC schemes is that the security of QKD does not rely on any computational assumptions. However, QKD protocols require specialized hardware for implementation. It possibly will need many years before building a global QKD network [14].

It has been also anticipated that QB can be conceptually designed as a quantum-networked time machine. This can be constructed using entanglement in time, where photons that have never coexisted can be entangled. The BC is encoded into a temporal Greenberger-Horne-Zeilinger (GHZ) state of photons that do not simultaneously coexist. The entanglement in time can provide a crucial quantum advantage and can be an interesting candidate for realizing the pure QB [15], [16]. Another proposal for "Quantum Bitcoin" utilizes quantum techniques for block mining and transaction verification on a classical BC ledger. This requires the use of quantum bit commitment protocols to be the alternative to digital signature schemes [13].

Furthermore, QBs that are based on quantum networks have also been explored. The classical data chains have been rebuilt using quantum states' correlation over entanglements [7]. Some other quantum cryptographic tools can also be beneficial in developing QBs. These might include, quantum random number generators, quantum authentication, quantum encryption, quantum fingerprints, and quantum money. Indeed, it is possible to consider a full QB based on a distributed architecture. In this architecture, the nodes would be quantum computers that are linked by quantum communication channels. However, a practical realization of such a full QB requires many years to come [14], [17].

5. QKD-based QB Schemes

Considering quantum information techniques, QKD is the most widely deployed protocol with security proof and a good level of technological maturity. QKD systems are already worldwide in the public and private sectors. For the time being, QKD is performed on private networks and is limited to metropolitan networks. This puts limits on the practicality of QKD for most applications. However, the technology is rapidly developing and it is envisioned that shortly it will get more widespread. Researchers have demonstrated that incorporating QKD into BC can make it more secure and robust. Other quantum techniques might be also helpful in this direction [3], [9]. This section aims to explore some QKD-based QB proposals in the literature.

A. Kiktenko et al. 2018 Scheme [11]

This QB proposal integrates QKD (for providing authentication) with a broadcast protocol that is based on Byzantine fault tolerance state-machine replication (without using digital signatures). An experimental demonstration of the scheme was implemented in an urban QKD network. The *n*-nodes QB network consists of two layers:

1. A QKD network's first layer enables the establishment of an information-theoretically secure secret key for each node pair.
2. A classical second layer that uses the created secret keys in the first layer for sending authenticated messages based on information-theoretically secure Toeplitz hashing.

For concreteness, the authors considered a QB that maintains a digital currency. The QB operation is performed in two phases; the creation of transactions and the construction of blocks for aggregating new transactions. Besides authentication using QKD, new blocks are added using a broadcast protocol that achieves information-theoretical security. The blocks are created in a decentralized fashion using the Shostak-Lamport-Pease protocol. This protocol can achieve a Byzantine agreement in a pairwise authenticated network given that there are less than $n/3$ dishonest parties.

B. Sun et al. 2019 Scheme [18]

One of the major limitations of Kiktenko et al. QB scheme is the efficiency of its adopted consensus protocol. When the number of cheating parties goes large, the protocol becomes

DOI:http://doi.org/10.24086/cocos2024/paper.1528

exponentially data-intensive. The Sun et al. 2019 scheme overcomes this limitation by proposing a consensus protocol that has only resources' quadratic dependence on the number of miners. This scheme is a framework of permissioned QB called Logicontract (LC). It adopts a QKD-based digital signature scheme and a vote-based consensus algorithm for achieving consensus on the QB. LC uses the Toeplitz hash-based message authentication code to achieve an unconditionally secure digital signature scheme. This authentication scheme uses the Toeplitz matrix that is generated by the secret key shared by Alice and Bob for hashing the message using matrix-vector multiplication. This is combined with encrypting the hash value using the one-time pad. LC signatures are generated based on the Toeplitz Group Signature (TGS), which is an integration of Toeplitz hash-based message authentication and a variant of the Amiri et al. signature scheme.

LC does not utilize a proof-based consensus protocol (such as the proof-of-work (PoW) used in Bitcoin). It rather deploys a vote-based consensus algorithm. This is more common in permissioned BCs. The LC's consensus algorithm is the Quantum-Secured Yet Another Consensus (QSYAC). This represents a variant of the Yet Another Consensus (YAC) algorithm, where the public-key signature is replaced by TGS.

C. Sun et al. 2020 Scheme [19]

Most QB systems present a general scheme for a distributed ledger. However, they usually do not offer specific protocols for tasks like voting, auction, or lottery that may be deployed on top of them. In order to demonstrate the power of QB, this scheme presented protocols for lottery and auction. The lottery protocol is defined for any number of players. It is also secured by a group of miners. In addition to the QB techniques used in the Sun et al. 2019 scheme, quantum bit commitment (QBC) is the main technique utilized to build the lottery and auction protocols here. This scheme leverages the previous QB scheme taking advantage of some of its desired properties, as follows:

- Every node is capable of performing the small-scale quantum computation required for the (QBC) protocol.
- The communication facility between various QB nodes is unconditionally secure.
- There is an immune-to-attacks algorithm for achieving consensus among miners

A bit commitment protocol typically consists of commitment and opening phases. In the first phase, Alice chooses a bit (0 or 1) and presents to Bob a piece of evidence about it. In the second phase, Alice discloses more information to Bob. This information enables Bob to reconstruct the original bit. A bit commitment protocol is concealing if Bob cannot know the bit before the opening phase. Indeed, it is a binding protocol if Alice cannot change the initial bit after the commitment phase. The no-go theorem by Mayers, Lo, and Chau implies that it is not possible to achieve unconditionally secure QBC within the quantum mechanics theory. Nevertheless, several ways have been found to overcome this negative result. For example, relativistic QBC protocols achieve unconditional security by making use of the relativity theory. This scheme used QBC to propose distributed lottery/auction protocols that can be implemented by the current technology.

D. Iovane 2021 Scheme [20]

This work represents a data transmission protocol based on combining the BB84 QKD protocol and BC. This enables the transmission of cryptographic keys in maximum security on quantum communication channels and/or on traditional channels emulating quantum functionalization. This proposal aims to extend the scope of BB84 beyond QKD based on a methodology particularly designed for BC and distributed ledgers. Instead of using a new encryption technique, this scheme achieves Computational Quantum Key Distribution (CQKD), which can operate not only on a physical quantum channel but also on channels with computational quantum components. Hence, the proposed methodology encourages the development of quantum nodes, and simultaneously the scheme can be deployed immediately on non-quantum nodes and channels. Each QB node can be in one of three states; off, busy, and active (i.e. idle and ready).

At first, Alice verifies the availability of QB nodes to receive the computational load required for key generation and transmission. Then, she proceeds to the nodes' functionalization stage. Each QB node can operate in one of six functions, which are Quantum Spin Generator, Base Generator, Quantum Photon Polarizer, Photon Fusion Engine, Quantum Photon Meter, and Quantum Photon Collider. As a result, the process of key generation can be considered for this setting as a mining process. This is because the key generation is done continuously and autonomously by the mining pool's nodes. The keys are produced at any time and immediately distributed whenever Alice and Bob need to exchange peer-to-peer messages.

In [21], the same author extended his proposal of CQKD proposed negotiation procedure for block validation and new block assignment in QB infrastructure. by using a novel negotiation procedure. The proposed approach combines complexity theory and quantum and relativistic mechanics to solve some important problems in the QB context, which are related to the fairness and randomness of block validation and the assignment of a new one.

E. Xu et al. 2023 Scheme [6]

This proposal is a framework of QB-driven Web 3.0 that provides unconditional security for decentralized data-transferring tasks and payment transactions. The continuous development of the QB-driven Web 3.0 consists of six main stages, as shown in Figure 2. At each stage, quantum cryptography techniques are used to support implementing the required protocols of that stage. These techniques include QKD, quantum secure direct communication (QSDC), quantum random number generators (QRNGs), quantum signature algorithms, quantum hash functions, and quantum voting protocols.

DOI:http://doi.org/10.24086/cocos2024/paper.1528

F. Sharma et al. 2023 Scheme [10]

In this QB proposal, QKD is used for distributing secret keys between nodes and also providing authentication. In general, QB uses the same components as the traditional BC. However, the major difference here is that, instead of using traditional public-key cryptography and hashing functions, QB utilizes quantum cryptography techniques to secure the network against various security threats including those from quantum computation. The workflow of the QB is shown in Figure 3. The proposed workflow consists of the following phases: Quantum transmission based on QKD, transaction proposal, transaction validation, quantum block proposal, and validation.

6. Challenges and Future Research Directions

Despite the interesting theoretical aspects of the QKD-based QB proposals so far, a lot has to be done before reaching real-world operating QB infrastructures, especially for large-scale networks. One can notice that the research on QB is still less, and there are many problems to be studied and analyzed. In this section, we discuss the research challenges and open problems for future research in QB technology. These can be summarized as follows:

a. Scalability: Scalability represents a concern in various quantum cryptography applications because of the current technology limitations. It is necessary to explore techniques to enhance the QB scalability for accommodating a larger number of nodes. For a full QB, complex quantum data structures need to be developed.

b. Standardization and Interoperability: It is important to develop widely accepted standards and protocols for ensuring QB interoperability and its seamless integration with current network technology. For the time being, more standardization efforts are needed for QB technology in general and for QKD-based QB infrastructures in particular.

c. Security Modeling and Risk Assessment: Researchers need to conduct thorough security modeling and risk assessments for various QB approaches. This is crucial for identifying potential attack vectors within the QB framework. Various possible quantum and classical attack scenarios must be simulated and analyzed to identify potential security vulnerabilities. In this respect, investigating privacy issues within the QB framework is also necessary.

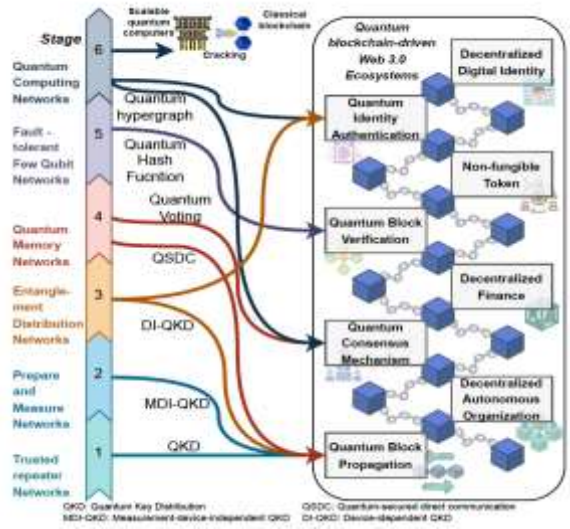

Figure 2 The stages of QB-driven Web 3.0 development [6].

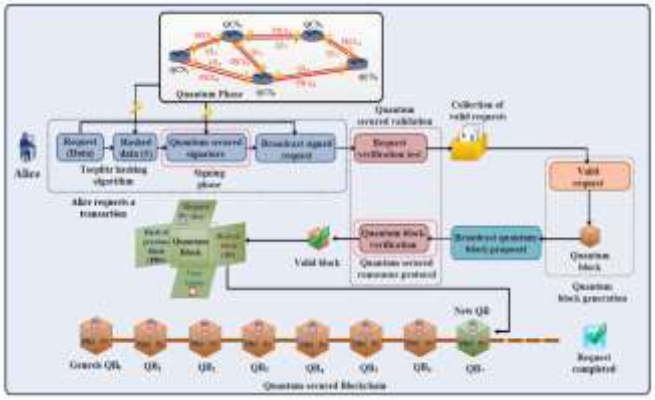

Figure 3 The process of the proposed QB [10].

d. *Network Overhead and Throughput:* Overhead in QB networks is significantly increased because the signatures are done interactively. Indeed, many quantum-based signatures can only be validated once. Hence, the number of the required signature processes would significantly increase and also the overhead. network nodes. Some researchers envisioned that using quantum fingerprints instead of interactive signatures can solve this issue, but quantum fingerprint schemes still need more investigation. Other schemes have also proposed to improve throughput for QB. However, QB network resources are still limited and insufficient to satisfy the required large-scale throughput.

e. *Consensus Protocols:* In QB, the consensus method significantly affects the transaction speed, level of security, and network scalability. A consensus protocol enables every node in the QB network to agree on the current state of the shared distributed ledger. Only a few consensus protocols have been proposed for QB. Most currently used consensus protocols are still primitive. For example, QRNG which is sometimes used as a basic consensus method cannot guarantee the QB network's normal

DOI:http://doi.org/10.24086/cocos2024/paper.1528

operation. Furthermore, Byzantine agreement protocols become exponentially data-intensive when there is a large number of cheating nodes in QB. Therefore, serious research efforts are needed to develop new consensus protocols for QB.

f. *Trust:* The trust in the BC is built using digital signatures that serve as cryptographic proof primitives. However, in the case of QB, more research is required to develop quantum-based signature constructions that facilitate the establishment of trust in the QB network.

g. *Verification Schemes:* Participants in QB need to perform verification tests to check the transactions' validity. Therefore, in order to increase the security and reliability of the QB network, suitable verification schemes have to be proposed.

h. *Real-world Implementation and Validation:* Real-world QB systems need to be implemented and validation of the framework should be conducted based on these implementations. This might involve pilot deployments and performance evaluations in order to assess the QB security, practicality, and effectiveness in real-world scenarios.

i. *Cost:* Finally deploying cost-effective QB networks is one of the biggest challenges from the network architecture's perspective. Thus, it is necessary to build cost-efficient solutions for QB optical networks.

7. Conclusion

BC is a computational data structure that can provide an open, public, and distributed ledger. This has shown to have many promising applications. However, any cryptographic system must take into account the technological development anticipated to happen within its deployment lifespan. Hence, this work explores the vulnerabilities of BC networks to an adversary equipped with a quantum computing facility. Indeed, we have reviewed some interesting works that have been commenced on developing QB. These are expected to effectively resist or weaken the quantum attacks. Despite the current research efforts for developing secure and robust QB networks, more significant methods need to be investigated to develop large-scale real-world quantum-resistant systems. As future work, issues and challenges of designing PQC-based QB networks will be our focus in a subsequent paper.

8. References

[1] Rakesh Saini, Abhiprada Bera, Bikash K. Behera, Emad A. Ahmed, Mona Jamjoom, and Ahmed Farouk, "Designing quantum blockchain system integrated with 6G network," Journal of King Saud University - Computer and Information Sciences, Vol. 35, 101847, 2023. https://doi.org/10.1016/j.jksuci.2023.101847

[2] Shalini Dhar, Ashish Khare, Ashutosh Dhar Dwivedi, and Rajani Singh, "Securing IoT devices: A novel approach using blockchain and quantum cryptography," Internet of Things, Vol. 25, 101019, 2024. https://doi.org/10.1016/j.iot.2023.101019

[3] Wei Cui, Tong Dou, and Shilu Yan, "Threats and Opportunities: Blockchain meets Quantum Computation," *39th Chinese Control Conference (CCC)*, Shenyang, China, 2020, pp. 5822-5824, doi: 10.23919/CCC50068.2020.9189608.

[4] Wazir Zada Khan, Qurat-ul-Ain Arshad, Mudassar Raza, and Muhammad Imran, "Quantum Cryptography a Real Threat to Classical Blockchain: Requirements and Challenges," TechRxiv, October 24, 2022. DOI: 10.36227/techrxiv.21341817.v1

[5] Sufyan T. Faraj, "A Novel Extension of SSL/TLS Based on Quantum Key Distribution," Proceedings of the International Conference on Computer and Communication Engineering (ICCCE08), Vol. I, pp. 919-922, Malaysia, May 13-15, 2008.

[6] Minrui Xu et al., "When Quantum Information Technologies Meet Blockchain in Web 3.0," in IEEE Network, May 2023. doi: 10.1109/MNET.134.2200578.

[7] Zebo Yang, Tara Salman, Raj Jain, and Roberto Di Pietro, "Decentralization Using Quantum Blockchain: A Theoretical Analysis," IEEE Transactions on Quantum Engineering," Vol. 3, 4100716, 2022. DOI: 10.1109/TQE.2022.3207111.

[8] Sufyan T. Faraj Al-Janabi, "Quantum Key Distribution Networks," in Multidisciplinary Perspectives in Cryptology and Information Security, Sattar Sadkhan and Nidaa Abbas, Eds., IGI Global, 2014, ISBN13: 9781466658080.

[9] Brandon Rodenburg and Stephen P. Pappas, "Blockchain and Quantum Computing," MITRE Technical Report, MTR170487, Princeton, NJ, June 2017.

[10] Purva Sharma, Kwonhue Choi, Ondrej Krejcar, Pavel Blazek, Vimal Bhatia, and Shashi Prakash, "Securing Optical Networks Using Quantum-Secured Blockchain: An Overview," Sensors, Vol. 23, 1228, 2023. https://doi.org/10.3390/s23031228

[11] E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.I. Lvovsky, and A.K. Fedorov, "Quantum-secured blockchain," Quantum Science and Technology, Vol. 3, No. 3, 035004, 2018. DOI: 10.1088/2058-9565/aabc6b

[12] Rahul Saha, Gulshan Kumar, Tannishtha Devgun, William J. Buchanan, Reji Thomas, Mamoun Alazab, Tai Hoon-Kim, and Joel Rodrigues, "A Blockchain Framework in Post-Quantum Decentralization," IEEE Transactions on Services Computing, vol. 16, no. 1, pp. 1-12, 1 Jan.-Feb. 2023, doi: 10.1109/TSC.2021.3116896.

[13] Chao-Yang Li, Xiu-Bo Chen, Yu-Ling Chen, Yan-Yan Hou, and Jian Li, "A New Lattice-Based Signature Scheme in Post-Quantum Blockchain Network," IEEE Access, Vol. 7, 2019, pp. 2026-2033. DOI: 10.1109/ACCESS.2018.2886554

[14] Vlad Gheorghiu, Sergey Gorbunov, Michele Mosca, and Bill Munson, "Quantum-Proofing the Blockchain," foreword by Don Tapscott, Blockchain Research Institute, 23 Nov. 2017.

[15] Del Rajan and Matt Visser, "Quantum Blockchain Using Entanglement in Time," Quantum Reports, Vol. 1, No. 1, 2019, pp. 3-11. https://doi.org/10.3390/quantum1010002.

[16] Yu-Long Gao, Xiu-Bo Chen, Gang Xu, Kai-Guo Yuan, Wen Liu, and Yi-Xian Yang, "A novel quantum blockchain scheme base on quantum entanglement and DPoS," Quantum Information Processing, Vol. 19, 420, 2020. https://doi.org/10.1007/s11128-020-02915-y

[17] Wusheng Wang, Yang Yu, and Lingjie Du, "Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm," Scientific Reports, Vol. 12, No. 1, 2022, pp. 1-12. https://doi.org/10.1038/s41598-022-12412-0

[18] Xin Sun, Mirek Sopek, Quanlong Wang, and Piotr Kulicki, "Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic," Entropy, Vol. 21, 887, 2019. DOI:10.3390/e21090887

[19] Xin Sun, Piotr Kulicki, and Mirek Sopek, "Lottery and Auction on Quantum Blockchain," Entropy, Vol. 22, 1377, 2020. DOI:10.3390/e22121377.

[20] Gerardo Iovane, "Computational quantum key distribution (CQKD) on decentralized ledger and blockchain," Journal of Discrete Mathematical

Sciences and Cryptography, 27 April 2021. DOI: 10.1080/09720529.2020.1820691.

[21] Gerardo Iovane, "MuReQua Chain: Multiscale Relativistic Quantum Blockchain," IEEE Access, Vol. 9, 2021, pp. 39827-39838. DOI: 10.1109/ACCESS.2021.3064297

DOI:http://doi.org/10.24086/cocos2024/paper.1528