

# Quantum Blockchain Survey: Foundations, Trends, and Gaps

Saurav Ghosh

Southeast Missouri State University

Cape Girardeau, Missouri, USA

sghosh3s@semo.edu

## Abstract

Quantum computing poses fundamental risks to classical blockchain systems by undermining widely used cryptographic primitives. In response, two major research directions have emerged: post-quantum blockchains, which integrate quantum-resistant algorithms, and quantum blockchains, which leverage quantum properties such as entanglement and quantum key distribution. This survey reviews key developments in both areas, analyzing their cryptographic foundations, architectural designs, and implementation challenges. This work provides a comparative overview of technical proposals, highlight trade-offs in security, scalability, and deployment, and identify open research problems across hardware, consensus, and network design. The goal is to offer a structured and comprehensive reference for advancing secure blockchain systems in the quantum era.

## 1 Introduction

Quantum technologies are moving fast, and two of the most talked-about areas are the quantum internet and quantum blockchain. Both are still in early stages, but the ideas behind them could reshape how we think about secure communication, distributed systems, and trust. The quantum internet aims to connect quantum devices using entanglement and other quantum effects, while quantum blockchain tries to build tamper-proof ledgers using quantum principles or protect existing systems from quantum attacks.

There's a lot of work happening in both areas, but much of it is still experimental or theoretical. At the same time, these fields are closely related: quantum networks could provide the foundation for secure blockchain communication, and blockchains could help organize distributed quantum systems. Still, there are many open questions. How do you build reliable routing for entanglement? Can we design consensus without classical trust assumptions? How do we layer security in a quantum-native stack?

In this review, a small set of papers will be focused, where each tackles a part of this broader problem. Some propose new blockchain models based on quantum effects, others look at quantum routing or layered security models. Each of them brings a different idea to the table. The goal is not just to explain what each paper says, but to look at how these ideas connect, what assumptions they make, and what gaps still exist.

## 2 Backgrounds

This section covers the key technical foundations needed to understand the systems discussed in this review. It introduces the core quantum primitives, the basic structure of quantum networks, and why integrating blockchain with quantum infrastructure has become an important research direction.

### 2.1 Quantum Primitives

Quantum entanglement is a key resource in both quantum communication and computation. It allows for correlations between particles that are stronger than anything classical systems can achieve. This property enables quantum key distribution (QKD), where two parties can share encryption keys with provable security based on quantum physics. QKD has been implemented over fiber and satellite links, but it still faces distance and throughput limitations.

While QKD protects against many types of attacks, it does not replace the need for digital signatures and consensus mechanisms. This is where post-quantum cryptography (PQC) comes in. PQC uses classical algorithms—like lattice-based or hash-based schemes—that are designed to resist attacks from quantum computers running algorithms such as Shor's. These schemes are being standardized, but they often come with trade-offs in key size, signature length, or computational cost.

Entanglement and QKD are critical to how information is shared securely in a quantum network, while PQC focuses on protecting classical data from quantum attacks. These tools together shape how quantum and classical security models can work in parallel or be combined.

### 2.2 Quantum Networks

A quantum network is made up of nodes connected by links that distribute entangled qubits. These links can be optical fibers or satellite connections, and the network may include quantum repeaters to extend distances. Information isn't sent directly as data packets like in classical networks—instead, the goal is to create and maintain entanglement across the network, which can then be used for teleportation, secure key exchange, or distributed quantum computation.

The control plane of a quantum network coordinates entanglement generation, path selection, and resource management. This introduces unique challenges: entanglement is fragile, cannot be copied, and often decays quickly. As a result, routing and scheduling in quantum networks must deal with probabilistic link behavior and physical constraints that do not appear in classical systems.

Designing scalable quantum networks also means thinking in layers—similar to how the classical internet has protocol stacks. Efforts are underway to define such layered architectures, often drawing from software-defined networking (SDN) and classical internet design patterns, but adapted to quantum-specific requirements.

### 2.3 Integration Drivers

The idea of combining blockchain systems with the quantum internet is driven by the limitations of current distributed systems and the expected capabilities of future quantum infrastructure.

Blockchains rely on consensus protocols and cryptographic primitives that are vulnerable to quantum attacks. At the same time, blockchains often assume trusted channels or delay-tolerant networks, which quantum communication could potentially improve.

On the other side, distributed quantum systems will eventually need mechanisms for coordination, auditability, and decentralized trust—goals that blockchain systems are already designed to support. Bringing these together opens up interesting design spaces: for example, using QKD to secure blockchain transactions, using quantum entanglement to prove timestamp integrity, or applying blockchain logic to organize entanglement routing and resource allocation.

This overlap has led researchers to explore hybrid systems, quantum-native blockchain models, and layered security architectures that treat blockchain and quantum networks as complementary technologies rather than separate domains.

### 3 Thematic Analysis of Quantum Blockchain

To better understand the research landscape in quantum blockchain, this section groups the key papers based on shared technical ideas and system designs. Instead of reviewing each work individually, we focus on the recurring themes that shape this field—such as the use of entanglement, quantum-secured consensus, hybrid architectures, and quantum routing. This thematic approach will make it easier to compare different directions and identify where future work is needed.

However, before going into the details of each work, it helps to have a quick view of what each paper focuses on and where its main contributions and limitations lie. Table 1 summarizes the core set of papers covered in this review. This includes both foundational ideas and more recent proposals, spanning different parts of the broader quantum stack.

The table is organized to show each paper’s area of focus, the key ideas it introduces, and the challenges it leaves open. This overview is meant to provide context for the sections that follow, where each work is examined in more detail and discussed in relation to others.

#### 3.1 Foundations and Limitations

Blockchains store records in a chain of blocks, where each new block references the hash of the previous one [37]. This design prevents tampering, as modifying one block requires changing all subsequent blocks. Classical blockchains rely on public-key cryptography and one-way hash functions. However, both are vulnerable to quantum algorithms—Shor’s algorithm can factor large numbers in polynomial time [1], and Grover’s algorithm offers quadratic speedups for brute-force search [39]. A large enough quantum computer could forge signatures or find hash collisions easily [2], which threatens blockchain integrity. These concerns highlight the need to explore solutions that can withstand quantum attacks.

A quantum blockchain uses quantum information to achieve ledger security [3]. This is not a simple upgrade. It involves methods such as quantum key distribution (QKD) [4–6] and entangled states to detect tampering and handle trust among distributed nodes. So far, these ideas exist mostly in theoretical research and small-scale tests [3, 7–9], but they promise a way to secure blockchains against future quantum threats.

**3.1.1 Classical Cryptographic Vulnerabilities:** Firstly, there is a public-key cryptography vulnerability. Systems like RSA or ECDSA assume that factoring large numbers is extremely hard. Shor’s algorithm can factor these in polynomial time [1], which weakens the security of digital signatures and may eventually allow attackers to sign transactions they do not own.

Secondly, there is the hash function weakening issue. Hashing prevents unauthorized changes to data because it is costly to find two inputs that produce the same output. Grover’s algorithm provides a quadratic speedup for brute-force attacks [39], weakening standard hash security and making brute-force collision finding much faster than before.

Thirdly, there is a consensus impact. Quantum computers may compute proof-of-work (PoW) puzzles more quickly [10, 11], which introduces vulnerabilities such as 51% attacks (in PoW or PoS), quantum key theft (breaking RSA/ECDSA), and replay attacks. These are all possible to some extent under classical blockchain assumptions.

If the above concerns are not handled carefully, classical blockchains can no longer guarantee safe transactions in the future. An attacker with a powerful quantum computer could rewrite parts of the ledger, forge ownership, or compromise consensus protocols. A visual summary of this progression is shown in Figure 1.

**3.1.2 Key Components:** Although quantum blockchain designs vary, most share the following components:

**Quantum-Resistant Cryptography:** Since traditional methods may be broken by quantum computers, post-quantum cryptography—such as lattice-based or error-correcting code-based approaches—is proposed [12, 13]. Another strategy is to use fully quantum approaches like quantum keys and one-way transformations that are impossible to reverse without a trapdoor [3, 7–9].

**Entangled State Storage:** Some designs propose linking blocks through entangled quantum states such as GHZ states. This means that if a block is entangled with the previous one, any tampering would collapse the entanglement and be instantly detectable [14–16].

**New Consensus Mechanisms:** In a quantum blockchain, consensus needs to be reimaged. Instead of mining or staking, some systems use quantum random number generators [17] to ensure true unpredictability in block selection. Others propose interactive verification tests, where multiple nodes validate quantum-generated blocks collaboratively [3, 7–9].

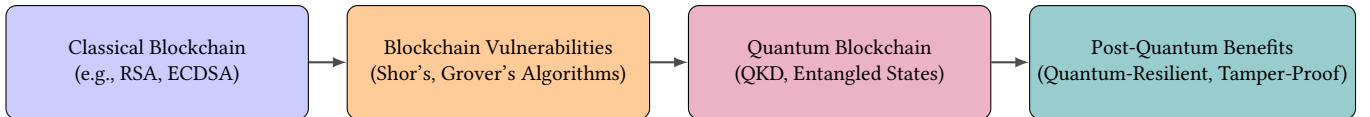
**Quantum Network Challenges:** Running a quantum blockchain is not just a software problem—it requires specialized hardware. Real-world quantum networks depend on technologies such as photon-based repeaters or superconducting qubits. However, quantum states are fragile; noise and decoherence can degrade the quality of stored and transmitted data [4–6].

**3.1.3 Implementation Challenges:** Shor’s and Grover’s algorithms remain the most prominent threats to classical security [1, 39]. While some mitigation can be achieved by increasing key and hash lengths, this is unlikely to provide a long-term solution once scalable quantum hardware becomes available [2].

Current quantum processors are still early in development, often with only dozens or hundreds of qubits. IBM, for example, has systems with 127 qubits. These processors suffer from high error

**Table 1: Overview of Key Literature in Quantum Blockchain and Quantum Internet**

Reference	Area	Contributions	Limitations
Rajan & Visser (2019) [3]	Quantum Blockchain	Introduced entanglement-in-time concept for quantum ledger integrity	Implementation remains theoretical; lacks scaling architecture
Kiktenko et al. (2018) [8]	Quantum Blockchain Security	Hybrid design using QKD and classical blockchain primitives	Requires quantum communication infrastructure not widely available
Sun et al. (2019) [6]	Logic-based Quantum Blockchain	Integrated logic reasoning and quantum-enhanced signatures	No physical implementation; heavy reliance on untested consensus logic
Pant et al. (2019) [50]	Quantum Routing	Developed model for entanglement-based routing over quantum networks	High dependency on link reliability; synchronous coordination needed
Yang et al. (2024) [66]	Asynchronous Quantum Routing	Proposed DODAG-based routing using local state updates for entanglement paths	No real-world validation; assumes homogeneous node behavior
Shi & Qian (2020) [65]	Concurrent Entanglement Routing	Parallel entanglement routing design for high-throughput quantum networks	Link correlation and physical loss modeling not fully covered
Bernstein & Lange (2017) [12]	Post-Quantum Cryptography	Survey of lattice, hash-based, and code-based quantum-safe schemes	Trade-offs in key sizes and speed; unclear real-world performance
Xu et al. (2020) [29]	QKD Systems	Comprehensive analysis of QKD protocol security and device imperfections	Distance limitations; low throughput hinders global adoption
Yang et al. (2023) [25]	Quantum Computing Survey	Structured overview of quantum hardware, networks, cryptography, and ML	Lacks empirical data or case studies; mainly theoretical
Lo, Curty & Tamaki (2014) [63]	QKD Protocol Security	Formal security analysis of BB84 and decoy-based QKD implementations	Doesn't cover new QKD integration with quantum internet stacks
Tannu & Qureshi (2019) [19]	Quantum Hardware	Highlighted variability in qubit fidelity and performance-aware scheduling	Limited scalability; variability remains hard to mitigate in hardware



**Figure 1: A linear progression showing the evolution from classical blockchain to post-quantum benefits.**

rates, limiting their practical use [19, 20]. Nonetheless, hardware is improving, and the goal of building thousands or millions of stable qubits remains a central research focus.

Quantum states themselves are fragile and collapse when observed. Entangled states can lose consistency over time [21–24], which presents a serious challenge for blockchain designs that rely on entanglement. The verification process must avoid unintentionally destroying the very state being validated. Moreover, sustaining large-scale entanglement demands sophisticated quantum engineering.

Consensus over quantum channels introduces further complexity. Multi-party protocols may be needed, where nodes measure different parts of a quantum state with randomly chosen bases. The measurement results must align with expected patterns to confirm validity. This makes consensus more complex than in classical systems and raises concerns about performance and scalability.

**3.1.4 Critical Observations:** Quantum computing fundamentally shifts the assumptions behind blockchain security, but implementing a full quantum blockchain requires advanced physics. This includes stabilizing qubits and deploying quantum networks that can tolerate distance and noise. Many projects do not yet have the resources or expertise to realize such systems. Meanwhile, the classical blockchain community is well-established, whereas quantum blockchain development is still early-stage. Researchers must build prototypes and refine protocols without sacrificing speed, which will take time and significant investment.

Some research papers inaccurately describe Shor’s (1994) and Grover’s (1996) algorithms as “recent advances,” despite their age. The true concern is the increasing pace of hardware progress. Moreover, several papers overlook critical issues like state stability and scalable quantum consensus. Quantum blockchains require enormous computational resources and coordination, which can limit

adoption even among large organizations. A clearer treatment of these concerns would provide a more balanced view.

Quantum computers will almost certainly compromise traditional blockchain security. To address this, post-quantum cryptography and quantum-native designs must be actively explored. Both offer promise, but also face significant engineering and design challenges. Entangled ledgers, quantum-proof signatures, and reimagined consensus mechanisms are theoretically compelling, but remain unproven at scale. For now, research continues at the intersection of theoretical innovation and small experimental systems. By preparing early, the field aims to avoid a disruptive crisis when quantum attacks become viable.

### 3.2 Computing & Networking Challenges

A broad overview of quantum computing and communications from a computer science perspective [25] is essential to understanding the field. Therefore, it is important to explore four key areas that are expected to form the future of the quantum Internet: quantum computers, quantum networks, quantum cryptography, and quantum machine learning. This section discusses their historical development and addresses major questions related to feasibility, performance, and security. Table 2 summarizes the core technical challenges and current status across these subfields, highlighting their interdependence in realizing a scalable and secure quantum infrastructure.

**3.2.1 Complexity of Quantum Research:** Quantum technologies have made rapid progress, with universal quantum computers now supporting hundreds of qubits and quantum annealers reaching thousands [26, 27]. Simultaneously, advances in quantum networking, cryptography, and machine learning have made the field more diverse. Without a structured guide, researchers and developers can easily become overwhelmed.

This work explains how quantum mechanics allows computation through principles like superposition and entanglement. It identifies key problems in building scalable and fault-tolerant quantum hardware [28], describes how quantum networks use entanglement, quantum repeaters, and specialized routing to connect quantum devices across distances [50], reviews quantum cryptographic techniques such as quantum key distribution (QKD) [29], and explores quantum machine learning applications, including how quantum computing can speed up optimization problems or improve data analysis through hybrid quantum-classical methods [30].

**3.2.2 Methodological Foundations:** Quantum computers offer exponential speed-ups through principles like superposition and entanglement. However, noise and decoherence disrupt quantum states, and the number of available qubits remains too small for large-scale computations [19]. Error correction is also difficult, as maintaining fault tolerance while scaling up quantum processors poses a significant engineering challenge.

Quantum networks rely on entanglement distribution via Einstein-Podolsky-Rosen (EPR) pairs and quantum repeaters [31]. Connecting quantum devices over long distances is complex due to fragile

quantum states, signal loss, decoherence, and the challenge of building efficient repeaters [50]. Unlike classical signals, quantum information cannot be copied or amplified, necessitating new routing methods for probabilistic entanglement and teleportation.

**3.2.3 Quantum Cryptography:** Quantum computing threatens current cryptographic schemes like RSA and ECDSA, making quantum-safe alternatives essential.

**Post-quantum cryptography:** It relies on lattice-based or code-based techniques [12, 13].

**Quantum key distribution (QKD):** It ensures secure communication using quantum principles, as demonstrated in BB84 and E91 protocols [35, 41].

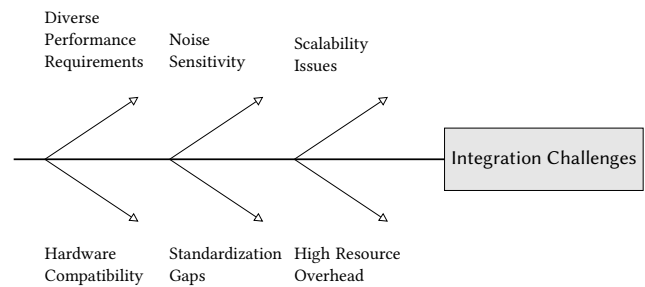
Other approaches, such as quantum signatures and coin-flipping, remain theoretical but highlight broader potential [36].

However, quantum cryptography has drawbacks. Despite theoretical unbreakability, real-world QKD systems face low key generation rates, DoS attack susceptibility, and operational distance limitations [29], all of which challenge its global practicality.

**3.2.4 Quantum Machine Learning:** Quantum hardware may accelerate tasks like large-scale optimization using quantum annealing and variational circuits. Quantum machine learning aims to enhance data analysis, while classical machine learning can optimize quantum experiments. However, today's quantum processors are too noisy and lack sufficient qubit connectivity for large, real-world datasets. Designing scalable, hybrid algorithms remains an open problem.

**3.2.5 Integration Challenges:** Integrating quantum computing, networking, cryptography, and machine learning into a unified system is a major challenge. Each subfield has different performance requirements, noise sensitivities, and hardware constraints. Ensuring system compatibility demands overcoming fundamental issues and developing standardized protocols.

While each subfield offers breakthroughs, the path to functional quantum networking remains difficult due to scalability, stability, and integration challenges. Figure 2 illustrates the integration issues briefly.



**Figure 2: Challenges in Integrating Quantum and Classical Systems**

**3.2.6 Open Research Questions: Quantum Hardware Constraints:** Quantum computers still have limited stable qubits. Noise and decoherence shorten coherence times, and low-temperature operation

**Table 2: Core Technical Challenges Across Quantum Subfields**

Subfield	Key Technical Challenge	Current Status
Quantum Hardware	High-fidelity multi-qubit operations, scalability, cryogenic control integration	Advancing via superconducting and trapped-ion platforms (IBM, Google, IonQ)
Quantum Networking	Stable long-distance entanglement distribution, quantum repeater deployment	Prototype networks under test; early QKD deployments in metropolitan areas
Quantum Cryptography	Efficient quantum key distribution (QKD), integration with classical infrastructure	Actively standardized (e.g., ETSI, ITU); limited real-world adoption
Quantum Machine Learning	Variational circuit stability, hybrid algorithm tuning on NISQ devices	Early-stage with limited scalability; constrained by hardware noise and data loading

is required [19]. Improved hardware is necessary to move toward practical systems.

**Networking Complexity:** Creating a global quantum Internet is difficult. Entanglement weakens over distance, and quantum routers must re-establish links continuously. No-cloning prohibits signal amplification, limiting scalability [32].

**Security Versus Performance Tradeoff:** Quantum computing threatens current cryptographic systems. While post-quantum methods exist, they may reduce performance and demand infrastructure overhauls [33].

**Quantum Machine Learning Limitations:** Quantum machine learning is promising but limited by current hardware and dataset compatibility. More research is required to realize practical applications [34].

Progress depends on strong theory, significant investment, and standards for integration. Quantum systems must be combined with classical infrastructure, which adds complexity beyond scientific research [28].

These works however lacks implementation detail. They does not fully explain quantum-classical interaction, especially error correction and hardware challenges. They also lacks a roadmap for scaling from prototype to large-scale systems.

A few real-world case studies are discussed as well. Although theoretical models are explored, practical examples or benchmarks are missing. Security discussions largely focus on well-known quantum attacks, omitting side-channel vulnerabilities and the deployment of post-quantum cryptography at scale.

The future of quantum computing depends on solving these limitations—advancing hardware, securing networks, and integrating with classical systems. Industry interest is growing, particularly in areas like quantum cloud services and QKD. With improvements in error correction, entanglement distribution, and post-quantum cryptography, a global quantum Internet may emerge within the next decade.

### 3.3 Post-Quantum vs. Quantum Blockchain

The main challenge facing blockchain technology is the rapid progress in quantum computing. In particular, the problems inherent in our current cryptographic and consensus systems need to be discussed before outlining how post-quantum and quantum blockchains can address these issues.

**3.3.1 Problem Identification:** Classical blockchains depend on public-key cryptography (such as RSA and ECDSA) and robust hash functions (like SHA-256) to secure transactions and maintain system integrity [37, 38]. However, quantum algorithms—most notably Shor’s algorithm [1] for factoring and Grover’s algorithm [39] for search—pose serious risks. Quantum computers can break these cryptographic methods. If an adversary uses Shor’s algorithm to factor large integers, they could derive private keys from public keys, thereby compromising the entire blockchain system.

**Consensus Vulnerabilities:** Blockchain networks rely on consensus mechanisms, such as proof-of-work, to validate transactions and maintain a decentralized ledger [37]. Quantum computing may allow an attacker to solve proof-of-work puzzles much faster than classical computers, potentially leading to a 51% attack. This disparity could let a malicious actor control the network, rewrite history, or disrupt the consensus process.

**Hardware and Networking Limits:** Current quantum hardware is still in its infancy—limited qubit counts, high noise levels, and rapid decoherence hamper practical large-scale computations. Additionally, while quantum key distribution (QKD) offers a secure means for exchanging keys, distributing entangled states over long distances is extremely challenging due to signal loss and the no-cloning theorem [40, 41]. Without scalable and stable quantum hardware and networking, fully quantum blockchain systems remain largely theoretical.

**Performance Trade-offs:** Replacing classical cryptography with post-quantum alternatives introduces performance challenges. Many post-quantum schemes require larger key sizes and more computation, which can slow down transaction processing and complicate integration with existing infrastructure.

**3.3.2 Solution Approaches:** After understanding the problems, the two main approaches to secure blockchain systems in a quantum era are outlined below.

#### *Post-Quantum Blockchains:*

- **What:** Replace vulnerable classical cryptographic primitives with quantum-resistant alternatives.
- **Why:** These rely on mathematical problems that are hard for quantum computers (e.g., lattice-based or code-based schemes) [12].

- **How:** For instance, lattice-based schemes based on the Shortest Vector Problem (SVP) or Learning With Errors (LWE) [42, 43] are proposed. They secure transactions but increase computational overhead.

#### *Quantum Blockchains:*

- **What:** Rebuild blockchain architecture using quantum technologies.
- **Why:** Employ QKD, quantum digital signatures, and quantum data structures for security grounded in quantum mechanics [44, 45].
- **How:**
  - **Hybrid Quantum Blockchains:** Combine classical infrastructure with quantum techniques (e.g., QKD) [46].
  - **Fully Quantum Blockchains:** Represent each block as a quantum state linked by entanglement [45]. Practical deployment remains constrained by current hardware.

**3.3.3 Issue Significance:** These problems strike at the core of blockchain trust:

- If cryptographic methods fail, the trust model collapses.
- A compromised consensus mechanism undermines decentralization.
- Limitations in current quantum technology hinder practical deployment.
- Performance trade-offs discourage the adoption of new cryptographic methods.

A clear understanding of these issues is critical. Whether upgrading classical systems with post-quantum cryptography or developing quantum-native blockchains, addressing these problems is key to securing decentralized systems in the quantum era.

## 3.4 Quantum Internet Routing Challenges

As we know, the future of the Computing Industry will be in Quantum Computing, and as a by-product, a lot of work is already going on in the Quantum Internet sphere [47–49, 61, 62]. However, for efficiency on the Internet, we need advanced quantum networking techniques that have significantly risen. Routing quantum entanglement without relying on fixed time slots is a big challenge because quantum links are really unpredictable and short-lived [50, 51]. Traditional methods that use synchronized time slots can waste resources because entanglement doesn't always happen at the right time. Therefore it is important to explore asynchronous routing, which means that the network updates its connections in real-time rather than following a fixed schedule. Quantum repeaters play an important role here, as they help extend entanglement over long distances [52, 53]. However, these repeaters are fragile as well, and entanglement swapping is not always successful. The best way to connect two distant nodes is to let each part of the network make local decisions as soon as entanglement becomes available. I felt this can justify a better use of quantum resources and therefore improve the chances of successfully routing entanglement over long distances. Finally, the most important more here is: What is the best way to connect two remote nodes when each quantum link is probabilistic and has a limited lifetime?

**3.4.1 Asynchronous Quantum Routing Complexity:** The problem here is very practical. Quantum networks need to create connections over long distances using repeaters. Traditional methods use synchronized time slots, where all nodes try to create and swap entanglement at the same time. But this wastes many entangled pairs because not all attempts succeed. Since quantum states disappear quickly [57], wasted entanglement makes the network inefficient. A better way would be an asynchronous approach, where each node updates its connections independently based on local information. This is like how classical networks find paths using distributed graphs. With this method, quantum networks can save resources and improve their chances of creating stable connections over long distances.

**3.4.2 Asynchronous Routing Techniques:** This work has been built on three main components, as illustrated in Figure 3. First, it uses quantum repeaters which generate entangled pairs over direct links between adjacent nodes. These repeaters do entanglement swapping so that a connection between distant nodes can be built from many short links [60]. Second, it introduces a system that keeps an ongoing update of these connections in a network graph, which can be a destination-oriented directed acyclic graph (DODAG) or a spanning tree. Instead of waiting for all nodes to update together, each node independently updates its status based on what it sees around it [58, 59]. Third, the approach mixes quantum operations (like creating and swapping entanglements) with classical operations (i.e., sending out routing information). Nodes listen for connection requests and use their local network information to choose the next node to connect with. This method saves unused entanglements for future use and avoids making all nodes act at the same time.

This approach is built on many well-known ideas as well. For instance, the concept of quantum-native repeaters was introduced by Briegel *et al.* [52] and further studied in some later works [53, 54]. The idea of using distributed graph structures for routing is taken from classical networking research [55, 56].

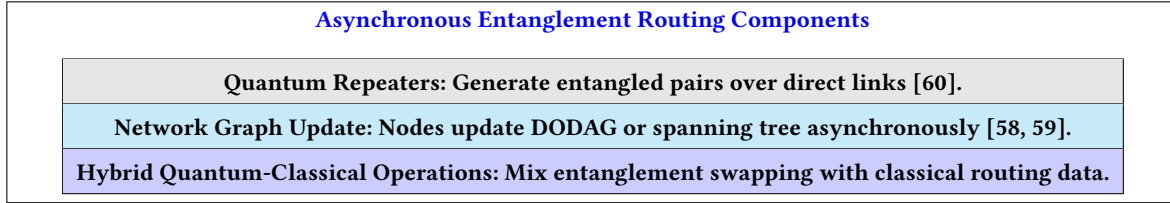
**3.4.3 Components and Challenges:** Each node in the network tries to create a quantum link with its neighbors, succeeding with a chance indicated by the parameter  $p$ . Swapping connections at intermediate nodes, needed to extend the link further, also has a success rate, represented by  $q$ . Nodes only know what's happening with their direct connections, which complicates finding the best path across the whole network. They solve this by updating a shared map of connections on their own, using only local data. Whenever a node needs to extend the connection, it uses this map to decide where to send the request next.

The big challenges here are the unpredictability of quantum operations because, as we know, the connections can fail to establish or drop unexpectedly and the fact that quantum links don't last long. Also, delays in updating the map can cause the route decisions to be based on old, incorrect information. Lastly, since each node updates its own map, the system has to be smart about avoiding loops and dead ends. The design takes ideas from classical distributed routing algorithms [50, 51] to avoid these issues.

The asynchronous approach can significantly improve the entanglement rate compared to synchronous methods. In synchronous protocols, all nodes are forced to use up available entanglements at

Characteristic	Classical Blockchain	Quantum Blockchain	Post-Quantum Blockchain
<b>Security</b>	Vulnerable to quantum attacks (Shor, Grover)	Uses quantum cryptography (QKD, entanglement)	Resistant to quantum attacks (Lattice, Hash-based cryptography)
<b>Consensus</b>	Proof-of-Work / Proof-Of-Stake	Quantum-secured consensus (Quantum RNG, QKD)	Modified PoW/PoS with post-quantum cryptographic methods
<b>Performance</b>	High throughput in classical systems	Experimental, requires quantum resources	Higher computational cost due to larger key sizes
<b>Scalability</b>	Well-tested, mature infrastructure	Limited by quantum hardware challenges	Still emerging, performance improvements ongoing
<b>Implementation Readiness</b>	Fully deployed in real-world applications	Mostly theoretical, few small-scale experiments	Actively researched, partial real-world deployment

**Table 3: Comparison of Blockchain Approaches: Classical, Quantum, and Post-Quantum**



**Figure 3: Key Components of Asynchronous Entanglement Routing**

fixed times, which can lower the overall rate. With asynchronous routing, unused direct-link entanglements are preserved and can be reused in future routing attempts. This results in a higher upper bound for the entanglement rate. The improvement is even more noticeable when the coherence time increases. It is needless to say as soon as we see the quantum hardware advances and coherence times become longer [59], asynchronous routing protocols may become essential.

There are still open challenges, however. For example, this work assumes that all nodes and links are homogeneous. In real networks, link qualities and node performances vary widely. Also, while they showed simulation results on grid topologies, the performance on more irregular networks is not fully explored. Finally, they did not have a good discussion on the security aspects of the protocol. In a practical network, delays and asynchronous updates might open new vulnerabilities that might need some additional attention.

Apart from the open challenges, these work does not go into detail about how the classical update process integrates with the quantum operations. The delay in classical communication is a critical factor, and, given the short coherence times, it is much more difficult in the event of quantum operations; the protocol does not fully address how to mitigate this issue. Security concerns, for example, the risk of malicious behavior in an asynchronous environment, are not analyzed as well.

The introduction of an asynchronous entanglement routing protocol for quantum networks works by updating a shared network

graph using local information, making it both simple and effective. It outperforms traditional synchronous methods by saving entanglement resources and increasing the entanglement rate. However, further testing in real-world conditions is needed to account for differences in network components and potential security risks. Overall, this study is an important step toward a scalable and efficient Quantum Internet.

However, these works are important because by proposing an asynchronous entanglement routing protocol, they made a great contribution to the field of quantum networking. The idea of maintaining a distributed graph with local information is both simple and effective. This method shows a clear advantage over traditional synchronous approaches. However, it is also important to test the protocol under realistic conditions. In one line, this work can be considered a great step towards an efficient Quantum Internet.

### 3.5 Entanglement Distribution

Given that the future is in Quantum Computing, we need to improve end-to-end entanglement in large quantum networks. This paper has used a multi-tree routing method that builds several destination-oriented directed acyclic graphs (DODAGs) at the same time. This method works for different network layouts i.e., grids, barbells, and realistic networks such as ESnet and Internet2. It is needless to say, by using multiple trees instead of a single one, it is very much possible to get a better end-to-end entanglement rate. Based on the simulations illustrated, it can be seen that the multi-tree method

gives higher entanglement rates than both the single-tree method and the traditional synchronous methods [61, 62].

**3.5.1 Multi-Tree Quantum Routing Complexity:** The main problem in entanglement distribution is to create end-to-end entanglement over long distances. In a quantum network, nodes must swap entanglements using intermediate repeaters [52, 53]. In many methods, the routing is divided into two phases. In the external phase, nodes create direct entanglements with each other. In the internal phase, repeaters swap these entanglements to connect distant nodes [50, 65]. However, using fixed time slots in these two phases can waste entanglement because the quantum links are not stable and the results are unpredictable. It can easily be noticed however that, in an asynchronous method, where each node updates its own view in real-time, can make better use of the available entanglement.

**3.5.2 Background of Multi-Tree Routing:** This work has been built on their earlier asynchronous routing protocol [66]. They started by forming a tree-like structure from the available direct links. This tree may be a DODAG or a spanning tree. Each node uses only the local information it gathers from its neighbors, much like classical routing methods [55, 56]. Then, instead of using one tree, they formed several trees (a multi-tree or DODAG forest). With multiple trees, nodes in dense areas can choose the best path. This structure helps avoid long detours that occur when using a single central root. In their method, quantum operations (for entanglement generation and swapping) work together with classical operations (for exchanging routing messages) to keep the network graph updated [67, 68].

In these works, however, every node here tries to create a direct link with its neighbors. As noted in the previous one, the chance of success for each direct link is given by  $p$ , and the chance of success for entanglement swapping at a repeater is given by  $q$ . Each node only sees the links to its immediate neighbors. They then update a local map of the network, called the instant topology. When a node needs to forward a connection request, it looks at this map to choose the best next node. The main challenge is that quantum links are probabilistic and decay quickly. If the local map is not updated fast enough, the routing decision may use old information. Also, when many trees share the same area, loops, and redundant paths might occur. Our design uses simple rules, such as each node choosing only one parent per tree, to avoid these problems [50, 65].

It is also observed that the multi-tree approach gives better results than the single-tree method or the traditional synchronous routing. In synchronous protocols, all nodes swap entanglement at fixed times. This fixed schedule can use up all the available entanglements even when some links are not ready, which lowers the overall rate [50]. With an asynchronous multi-tree method, unused direct-link entanglements are saved for later use. This saves resources and raises the maximum achievable entanglement rate. The benefit becomes even clearer when the coherence time of the quantum links is longer [59].

As noted in the previous challenge, these works assume that all links and nodes are the same, but in real networks, they vary. Also, the simulations mainly use grid and barbell topologies. More tests are needed on irregular networks.

It is true that, through this multi-tree quantum routing, a promising way to improve end-to-end entanglement rates in large networks is established. The idea of using multiple DODAGs to form a distributed graph with local updates helps save entanglement and raises the overall rate. Further research that will deal with network heterogeneity and address the security concerns is needed, however.

## 3.6 Quantum Internet Security Models

As we know, the quantum internet holds great promise for secure communication and advanced computing. However, it also faces unique security challenges that must be solved to protect its Confidentiality, Integrity, and Availability (CIA). Features like superposition bring new types of vulnerabilities that do not exist in classical networks. Related previous papers did not discuss security issues; however, this paper looks at the security challenges in the different layers of the quantum internet: the physical, link, network, and application layers. They have, however, used only the vulnerabilities and mitigation techniques that have been reported in the literature to build a framework that mixes classical and quantum methods for protecting the network [62, 63].

**3.6.1 Security Challenges in Internet:** Quantum mechanics gives us benefits such as the no-cloning theorem and measurement-induced disturbance, which help detect eavesdropping [41]. On the other side, these same features create new challenges. For example, while Quantum Key Distribution (QKD) can offer unconditional security, it can still be attacked by methods such as Photon Number Splitting (PNS) and Trojan-horse attacks [73, 74]. This work has found out that even though quantum protocols promise very high security, the hardware is often noisy and the classical channels used for control and routing may add extra weaknesses. This layered nature of the quantum internet makes it necessary to study security risks at every level.

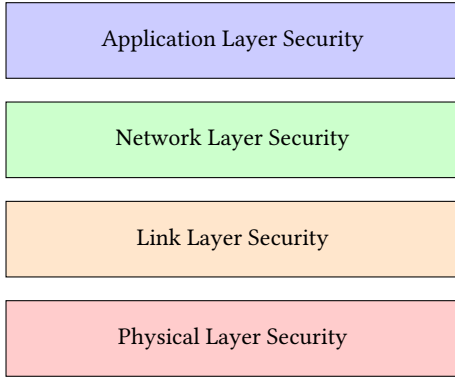
The approach in these studies was to break down the quantum internet into layers, much like the classical network protocol stack. They have identified the following layers:

- The **physical layer** > Quantum memories and the transmission media.
- The **link layer** > Handles the direct transmission of qubits and the operations of quantum repeaters.
- The **network layer** > Deals with the routing of entanglement.
- The **application layer** > Supports quantum applications such as QKD, quantum teleportation, and distributed quantum computing [79].

It is very important to discuss the main components at each layer, as illustrated in Figure 4 and the specific attacks that target them. It is also very important to review the mitigation techniques that others have proposed.

**3.6.2 Components and Challenge:** These work breaks the security framework into 4 main layers. In the physical layer, the main challenges come from the fragile nature of quantum devices. Photon-based systems can be attacked by PNS or Trojan-horse methods [74, 80]. These attacks try to steal information by abusing imperfections in photon sources and detectors.





**Figure 4: Layer-Wise Security Framework for the Quantum Internet**

In the link layer, the focus is on the direct channels between nodes. Quantum repeaters are used to extend the range of entanglement. However, these repeaters can be attacked by methods such as entangling-probe attacks or even man-in-the-middle attacks if an attacker takes control of a node [52, 53].

In the network layer, the challenge is to route entanglement over complex network layouts. Many routing schemes use classical control that is synchronized across the network, which creates single points of failure. If, for example, an attacker can compromise a repeater or change routing messages, the end-to-end entanglement can be seriously affected [50, 65]. Finally, at the application layer, protocols like BB84 and entanglement-based QKD are vulnerable to advanced attacks. Even though these protocols have ways to detect eavesdropping, they still face side-channel attacks and timing errors [41, 63]. A brief version is illustrated in Figure 4.

A layer-wise analysis is very important to fully understand the security of the quantum internet. Each layer has its own set of challenges. For example, the physical layer is very much limited by hardware flaws and environmental noise, while on the other hand, the link and network layers face issues with synchronization and trust. The application layer must unite quantum and classical security models for sure. One key comment is that many attacks work because current quantum networks still depend on classical communication channels. In the near future, as soon as the quantum systems improve, it will be a much more complex and sophisticated task to design flexible security measures that handle both quantum and classical weaknesses [69, 77].

There are several open challenges however. Many current studies assume that network components are uniform, but real networks are not. Also, the security of routing protocols in an asynchronous environment is not yet fully proven, especially when attackers may exploit untrusted nodes [78]. Future work should develop dynamic security solutions that can adapt to network changes in real-time, much like what we see in the regular approaches.

One limitation worth mentioning here is that they do not fully integrate the fast-changing quantum states with the slower classical update processes. This delay in classical communication is a big problem because qubits lose their state quickly, and the framework does not completely solve this issue [69]. Also, while the framework

provides a useful layer-by-layer breakdown, it sometimes assumes ideal conditions. In real networks, components can be very different, and link qualities may vary. Finally, the paper does not include extensive experimental tests or detailed simulations on irregular network topologies.

In simple words, the quantum internet is a groundbreaking technology that has its own set of unique features, however, because of them, it also creates a new set of security challenges that need a detailed, layer-by-layer analysis. This work sets out a security framework that covers vulnerabilities at different layers and suggests possible countermeasures. It is needless to say that, the framework shows promise, however, more research is needed to refine these strategies and also someone needs to test them in real-world networks (which will be the hardest part). Lastly, developing adaptive and strong security measures is important to ensure the long-term integrity and reliability of the quantum internet for practical use.

## 4 Discussion

This review has outlined two main paths forward in blockchain security under quantum threats: post-quantum cryptographic upgrades and fundamentally quantum-native systems. While both directions are promising, neither is without deep technical and practical challenges. This section identifies open problems and highlights research areas that demand further attention.

### 4.1 Key Research Gaps

Despite recent progress, significant gaps remain:

- **Hardware Limitations:** Quantum blockchains require quantum memories, entangled state distribution, and error-corrected qubits—all of which remain experimental or unavailable at scale.
- **Routing Realism:** Most quantum routing models rely on idealized assumptions (e.g., perfect links, synchronized timing). Realistic simulations and testbeds are urgently needed.
- **Incentive Models:** Few papers explore economic or game-theoretic models for quantum consensus. The interaction between incentives, verification costs, and quantum randomness needs deeper exploration.
- **Cross-Layer Design:** Most current work focuses on individual protocol layers. Integrated approaches—considering quantum hardware constraints, security assumptions, and blockchain architecture—are rare.
- **Lack of Testbeds:** Experimental validation is minimal. Even hybrid quantum-classical blockchain prototypes are largely untested outside simulations.

### 4.2 Design Trade-offs

Post-quantum cryptographic schemes introduce computational and storage overhead, which may not be acceptable in low-latency or resource-constrained environments. Quantum blockchain designs, while theoretically secure, demand advanced hardware and suffer from limited throughput, poor scalability, and operational fragility. Researchers must explicitly weigh these trade-offs when designing protocols.

Future designs may benefit from hybrid architectures that combine:

**Table 4: Security Threats and Mitigation Strategies Across Quantum Internet Layers**

Layer	Security Risks	Mitigation Strategies
<b>Physical</b>	Qubit decoherence, thermal noise, photon loss, side-channel leakage from quantum hardware (e.g., emission timing, power traces)	Quantum error correction, low-temperature shielding, fault-tolerant design, side-channel-resistant hardware interfaces
<b>Link</b>	Interception of quantum states (quantum man-in-the-middle), channel tampering during entanglement distribution, measurement disturbance	Quantum authentication protocols, decoy-state QKD, entanglement purification, Bell-test-based link verification
<b>Network</b>	Malicious or compromised nodes disrupting entanglement routing, denial-of-service through entanglement flooding, manipulation of routing metadata	Quantum-aware routing (e.g., entanglement-aware Dijkstra), authenticated control-plane messages, multi-path redundancy, topology-aware monitoring
<b>Application</b>	Trojan-horse attacks (e.g., injecting light to extract info), delay/timing-based side-channel leakage, protocol misuse, impersonation	Device-independent quantum cryptography, quantum-safe digital signatures, randomized quantum handshake protocols, quantum APIs

- Classical infrastructure with post-quantum cryptographic primitives.
- Quantum key distribution or quantum random number generators with classical consensus models.
- Modular architectures that can evolve alongside hardware capabilities.

Such systems can act as transition stages before fully quantum blockchains become viable.

Thereby, this work propose a phased adoption strategy:

- (1) Transition classical blockchains to NIST-backed post-quantum cryptography.
- (2) Build testbeds for hybrid quantum-classical blockchains using QKD modules.
- (3) Invest in small-scale quantum consensus experiments using optical networks or simulators.
- (4) Establish open benchmarks and simulation frameworks for routing, consensus, and scalability under quantum constraints.

Quantum computing will eventually transform trust and security infrastructure. Whether via resilient mathematical schemes or quantum-native protocols, the blockchain community must prepare now. Building secure, scalable, and hardware-aware blockchain protocols will require not just new algorithms but also real-world validation, interdisciplinary collaboration, and significant investment in quantum infrastructure.

## 5 Conclusion

Quantum computing is no longer a distant possibility—it is an active and growing field with direct implications for digital trust systems. This paper has examined how classical blockchains, which rely on public-key cryptography and hash functions, are fundamentally vulnerable to quantum attacks. In response, two major directions have emerged: post-quantum blockchain designs that extend classical security with quantum-resistant cryptography, and quantum blockchain models that build security directly into the quantum layer using entanglement and QKD.

Through a review of foundational papers, this work has highlighted key technical proposals, common design patterns, and unresolved challenges in routing, consensus, scalability, and real-world deployment. The comparative analysis clarified the distinct trade-offs between post-quantum and quantum approaches, noting that while post-quantum solutions are more deployment-ready, quantum blockchains offer theoretically stronger guarantees but rely on hardware that is not yet scalable.

Moving forward, the field must address critical research gaps such as hardware-aware design, realistic simulation environments, cross-layer integration, and formal consensus models. Hybrid systems and phased deployments may serve as a bridge between classical and quantum-secure infrastructures.

In sum, preparing blockchain systems for the quantum era requires both cautious upgrades and bold experimentation. By identifying key vulnerabilities, surveying cutting-edge proposals, and outlining paths forward, this paper aims to support ongoing research that will shape the future of secure decentralized technologies.

## References

- [1] 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.
- [2] 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.
- [3] 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.
- [4] C. Simon, "Towards a global quantum network," *Nature Photon.*, vol. 11, pp. 678–680, 2017, doi: 10.1038/s41566-017-0032-0.
- [5] 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.
- [6] 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.
- [7] 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.
- [8] 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.

- [9] X. Sun, Q. Wang, P. Kulicki, and X. Zhao, "Quantum-enhanced logic-based blockchain I: Quantum honest-success Byzantine agreement and qulogicoi," 2018, arXiv:1805.06768, doi: 10.48550/arXiv.1805.06768.
- [10] T. Salaman, 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.
- [11] M. Nofer, P. Gommer, 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.
- [12] D. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, pp. 188–194, 2017, doi: 10.1038/nature23461.
- [13] T. M. Fernández-Caramés 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.
- [14] 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.
- [15] 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.
- [16] 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.
- [17] W. McCutcheon et al., "Experimental verification of multipartite entanglement in quantum networks," *Nature Commun.*, vol. 7, 2016, Art. no. 13251, doi: 10.1038/ncomms13251.
- [18] "Ethereum whitepaper," Ethereum.org, Accessed: Jun. 14. 2014. [Online]. Available: <https://ethereum.org/en/whitepaper/>
- [19] 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.
- [20] 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>
- [21] 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.
- [22] 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.
- [23] M. Nowakowski, "Quantum entanglement in time," in *Proc. AIP Conf. Proc.*, 2017, Art. no. 020007, doi: 10.1063/1.4982771.
- [24] D. Rajan, "Quantum entanglement in time," 2020, arXiv:2007.05969, doi: 10.48550/arXiv.2007.05969.
- [25] Z. Yang, M. Zolanvari, and R. Jain, "A Survey of Important Issues in Quantum Computing and Communications," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, 2023.
- [26] J. Chow, O. Dial, and J. Gambetta, "IBM Quantum Breaks the 100-Qubit Processor Barrier," 2021.
- [27] S. Roberts, "This New Startup Has Built a Record-Breaking 256-Qubit Quantum Computer," 2021.
- [28] D. J. Reilly, "Challenges in scaling-up the control interface of a quantum computer," in *Proc. IEEE Int. Electron Devices Meeting (IEDM)*, 2019, pp. 31.7.1–31.7.6.
- [29] F. Xu, X. Ma, Q. Zhang, H. Lo, and J. Pan, "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys.*, vol. 92, no. 2, 2020.
- [30] A. Perdomo-Ortiz, M. Benedetti, J. Realpe-Gómez, and R. Biswas, "Opportunities and challenges for quantum-assisted machine learning in near-term quantum computers," *Quantum Science and Technology*, vol. 3, no. 3, 2018.
- [31] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Rev. Mod. Phys.*, vol. 83, 2011.
- [32] Y. Chen et al., "An integrated space-to-ground quantum communication network over 4,600 kilometers," *Nature*, vol. 589, 2021.
- [33] M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?" *IEEE Security & Privacy*, vol. 16, no. 5, 2018.
- [34] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning," *Nature*, vol. 549, 2017.
- [35] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing*, 1984, pp. 175–179.
- [36] A. Broadbent and C. Schaffner, "Quantum cryptography beyond quantum key distribution," *Designs, Codes and Cryptography*, vol. 78, 2015.
- [37] Nakamoto, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008.
- [38] Johnson, D., Menezes, A., & Vanstone, S., *The Elliptic Curve Digital Signature Algorithm (ECDSA)*, International Journal of Information Security, 2001.
- [39] Grover, L. K., *A Fast Quantum Mechanical Algorithm for Database Search*, Proc. 28th Annual ACM Symposium on Theory of Computing, 1996.
- [40] Bennett, C. H. & Brassard, G., *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Theoretical Computer Science, 2014.
- [41] Ekert, A. K., *Quantum Cryptography Based on Bell's Theorem*, Physical Review Letters, 1991.
- [42] Ajtai, M., *Generating Hard Instances of Lattice Problems*, Proc. 28th Annual ACM Symposium on Theory of Computing, 1996.
- [43] Regev, O., *On Lattices, Learning with Errors, Random Linear Codes, and Cryptography*, Journal of the ACM, 2009.
- [44] Kiktenko, E. O., et al., *Quantum-Secured Blockchain*, Quantum Science and Technology, 2018.
- [45] Rajan, D. & Visser, M., *Quantum Blockchain Using Entanglement in Time*, Quantum Reports, 2019.
- [46] JPMorgan, *Research on a Quantum-Resistant Blockchain Network*, Cointelegraph, 2018.
- [47] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, pp. 1023, 2008.
- [48] N. Gisin and R. Thew, "Quantum communication," *Nature Photonics*, vol. 1, pp. 165–171, 2007.
- [49] P. Komar et al., "A quantum network of clocks," *Nature Physics*, vol. 10, pp. 582–587, 2014.
- [50] M. Pant, H. Krovi, D. Towsley, L. Tassiulas, L. Jiang, P. Basu, D. Englund, and S. Guha, "Quantum routing for the quantum internet," *npj Quantum Inf.*, vol. 5, p. 25, 2019.
- [51] K. Chakraborty, F. Rozpedek, A. Dahlberg, and S. Wehner, "Distributed routing in a quantum internet," arXiv:1907.11630, 2019.
- [52] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, pp. 5932–5935, 1998.
- [53] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, "Experimental entanglement swapping: Entangling photons that never interacted," *Phys. Rev. Lett.*, vol. 80, pp. 3891–3894, 1998.
- [54] A. Techebotareva, S. L.N. Hermans, P. C. Humphreys, D. Voigt, P. J. Harmsma, L. K. Cheng, A. L. Verlaan, N. Dijkhuizen, W. de Jong, et al., "Extending the reach of quantum communications using telecom wavelengths," *Phys. Rev. Lett.*, vol. 123, p. 063601, 2019.
- [55] R. Alexander, A. Brandt, J. P. Vasseur, J. Hui, K. Pister, P. Thubert, P. Levis, R. Struik, R. Kelsey, et al., "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC 6550, 2012.
- [56] R. G. Gallager, P. A. Humblet, and P. M. Spira, "A distributed algorithm for minimum spanning trees," *ACM Trans. Program. Lang. Syst.*, vol. 5, pp. 66–77, 1983.
- [57] C. L. Degen, F. Reinhard, and P. Cappellaro, "Quantum sensing," *Rev. Mod. Phys.*, vol. 89, p. 035002, 2017.
- [58] R. Beals, S. Brierley, O. Gray, A. W. Harrow, S. Kutin, N. Linden, D. Shepherd, and M. Stather, "Efficient distributed quantum computing," *Proc. R. Soc. A*, vol. 469, p. 20120686, 2013.
- [59] R. Van Meter and S. J. Devitt, "The path to scalable distributed quantum computing," *Computer*, vol. 49, pp. 31–42, 2016.
- [60] K. Azuma, K. Tamaki, and H.-K. Lo, "All-photonic quantum repeaters," *Nature Communications*, vol. 6, p. 6787, 2015.
- [61] S. Wehner, D. Elkouss, and R. Hanson, "Quantum Internet: A Vision for the Road Ahead," *Science*, vol. 362, no. 6412, p. eaam9288, 2018.
- [62] Z. Yang, M. Zolanvari, and R. Jain, "A Survey of Important Issues in Quantum Computing and Communications," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1059–1094, 2023.
- [63] H.-K. Lo, M. Curty, and K. Tamaki, "Secure Quantum Key Distribution," *Nature Photonics*, vol. 8, pp. 595–604, 2014.
- [64] S. Muralidharan et al., "Optimal Architectures for Long Distance Quantum Communication," *Scientific Reports*, vol. 6, p. 20463, 2016.
- [65] S. Shi and C. Qian, "Concurrent Entanglement Routing for Quantum Networks: Model and Designs," in *Proc. SIGCOMM '20*, New York, NY, USA: ACM, July 2020, pp. 62–75.
- [66] Z. Yang et al., "Asynchronous Entanglement Routing for the Quantum Internet," *AVS Quantum Sci.*, vol. 6, no. 1, Jan. 2024.
- [67] G. W. Furnas and J. Zacks, "Multitrees: Enriching and Reusing Hierarchical Structure," in *Proc. SIGCHI Conf.*, Boston, MA, USA: ACM, 1994, pp. 330–336.
- [68] P. Erdős and A. Rényi, "On Random Graphs," *Publ. Math. Debrecen*, vol. 6, pp. 290–297, 1959.
- [69] J. Preskill, "Quantum Computing in the NISQ Era and Beyond," *Quantum*, vol. 2, p. 79, 2018.
- [70] "About ESnet," ESnet; available: <https://www.es.net/about/>, accessed: Nov. 15, 2023.
- [71] S. Knight et al., "The Internet Topology Zoo," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 9, pp. 1765–1775, Oct. 2011.
- [72] "About Internet2," Internet2; available: <https://internet2.edu/community/about-us/>, accessed: Nov. 15, 2023.

- [73] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, pp. 1330–1333, 2000.
- [74] Y. Zhao, C. H. F. Fung, B. Qi, C. Chen, and H. K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A*, vol. 78, p. 042333, 2008.
- [75] X. Ma, B. Qi, Y. Zhao, and H. K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, p. 012326, 2005.
- [76] W. Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Phys. Rev. Lett.*, vol. 91, p. 057901, 2003.
- [77] T. Satoh et al., "Attacking the Quantum Internet," *IEEE Trans. Quantum Eng.*, vol. 2, pp. 1–17, 2021.
- [78] H. Inamori, "Security of EPR-based quantum cryptography against incoherent symmetric attacks," *J. Phys. A: Math. Gen.*, vol. 34, p. 6913, 2001.
- [79] J. Illiano, M. Caleffi, A. Manzalini, and A. S. Cacciapuoti, "Quantum Internet protocol stack: A comprehensive survey," *Comput. Netw.*, vol. 213, p. 109092, 2022.
- [80] C.-Y. Lu, Y. Cao, C.-Z. Peng, and J.-W. Pan, "Micius quantum experiments in space," *Rev. Mod. Phys.*, vol. 94, p. 035001, 2022.