Graphical Abstract

Quantum and Post-Quantum Blockchain: A Systematic Survey

Ruwanga Konara, Awansika Nimuthumana, Asanka Sayakkara, Anuradha Mahasinghe, Kasun De Zoysa

Author Email Addresses in the Order of Names

- ruwangathandulakonara@gmail.com
- awansikanimuthumana@maths.cmb.ac.lk
- asa@ucsc.cmb.ac.lk
- anuradhamahasinghe@maths.cmb.ac.lk
- kasun@ucsc.cmb.ac.lk

Highlights

Quantum and Post-Quantum Blockchain: A Systematic Survey

Ruwanga Konara, Awansika Nimuthumana, Asanka Sayakkara, Anuradha Mahasinghe, Kasun De Zoysa

- An extensive overview of the current state of the art in post-quantum blockchain and post-quantum blockchain.
- An extensive overview of the current state of the art in quantum blockchain.
- A critical analysis of quantum blockchains found in the literature

Quantum and Post-Quantum Blockchain: A Systematic Survey

Ruwanga Konara[a], Awansika Nimuthumana[a], Asanka Sayakkara[a], Anuradha Mahasinghe[b], Kasun De Zoysa[a]

, , , , ,

[a] *University of Colombo School of Computing, UCSC Building Complex, 35 Reid Ave, Colombo 07, Colombo, 00700, Western, Sri Lanka*
[b] *Department of Mathematics, Faculty of Science, University of Colombo, Colombo 03, Colombo, 00700, Western, Sri Lanka*

Abstract

This literature review explores the state-of-the-art advancements in quantum and post-quantum blockchain. The realm of quantum computing is on the rise and will disrupt entire tech industries, including classical cryptography, which is the foundation of blockchain. There has been extensive research on classical cryptosystems (i.e., post-quantum) and their integration with blockchain to create quantum-resistant classical blockchains. We have reviewed the state-of-the-art in these post-quantum blockchains in academic research. But to have forward compatibility with the quantum internet and infrastructure in the future and to have quantum mechanical security, research has been conducted to implement blockchain on quantum technologies and quantum cryptography as well. Consequently, we have explored the current state of research in these quantum solutions, known as quantum blockchains.

Keywords: Quantum computing, Post-quantum cryptography, Quantum cryptography, Blockchain, Lattice-based cryptography, Blockchain security, Quantum internet, Quantum key distribution, Quantum-resistant algorithm, Code-based cryptography

1. Introduction

Blockchain has emerged as a disruptive innovation, enabling decentralized, secure, and transparent systems for a wide array of applications. The first functional blockchains, the very first of which was the chain under Bitcoin, were cryptocurrencies. From those origins, blockchain has evolved to encompass diverse domains, including supply chain management, decentralized finance in fintech, healthcare, identity management, and the Internet of Things (IoT). Being a public ledger that stores data such as transaction records or event logs that is shared among a host of entities that do not necessarily trust each other, blockchain's reliance on cryptographic primitives—such as digital signatures and hash functions—ensures the integrity, authenticity, and immutability of data. However, the rapid development of quantum computing engenders a formidable threat to these foundational cryptographic elements, necessitating a re-evaluation of blockchain technology's security and design against quantum adversaries.

1.1. The Quantum Threat

The rise of quantum computing and the implementation of algorithms, such as Shor's and Grover's, has raised alarming concerns regarding the vulnerability of classical cryptographic systems and their components, like hash functions and signature schemes. Shor's algorithm can factorize large numbers on a quantum computer in polynomial time, undermining public-key cryptosystems like Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), which are widely used for digital signatures. Grover's algorithm accelerates unstructured searches, for instance, through a hash input space, reducing the complexity of breaking hash functions (finding collisions) from $O(n)$ to $O(\sqrt{n})$. These threats wreak havoc on blockchain technology's security, integrity, and trust.

1.2. Adapting Blockchain to the Quantum Era

In the last 15 years, two approaches to mitigate these risks and innovate in the process have been formulated by researchers: post-quantum blockchains and quantum blockchains. Both of these trajectories make blockchains immune to quantum invasions, but they are entirely different, even to the minute details.

Post-Quantum Blockchains

These solutions are entirely classical blockchains running on classical hardware and networks. Classical blockchains are adapted by replacing their cryptosystems with post-quantum classical cryptosystems. Post-quantum cryptosystem components are immune to known quantum attacks. These cryptosystems leverage mathematical problems, such as lattice-based, code-based, multivariate, and hash-based schemes, that are considered quantum-resistant. The fusion of post-quantum cryptography into blockchains involves re-engineering digital signatures, key exchange protocols, and other cryptographic processes to maintain security against quantum threats. Additionally, comparing these cryptosystems and their variants/derivatives from various literature in terms of performance, scalability, and security is critical for selecting the most suitable solutions for blockchain integration.

Quantum Blockchains

These novel, mostly conceptual, blockchains leverage quantum computing technologies to build and sustain blockchains on quantum computers, networks, and quantum communication channels. Quantum blockchains explore the use of Quantum Networks, Quantum Teleportation, Quantum Bit Commitment, Quantum Key Distribution (QKD), Quantum Signatures, and Quantum Hash Functions to create inherently secure systems. Harnessing quantum mechanical properties, such as entanglement and superposition, quantum blockchains are believed to be *unconditionally secure.* These quantum technologies enable blockchain developers to achieve consensus and security. Moreover, hybrid quantum blockchains, which combine classical and quantum components, pave the path for a transition toward fully quantum blockchains.

1.3. Scope and Structure of the Review

This review aims to log the state-of-the-art of both quantum and post-quantum blockchains via a comprehensive examination of both of these technologies, solidifying foundational knowledge while exploring their strengths, limitations, and future potential. The structure of this review is as follows.

Section 2 provides an adequate, comprehensive overview of classical cryptography, classical blockchain, and the threats posed by quantum computing upon them. It explores Shor's and Grover's algorithms and their implications on classical cryptographic elements such as signature schemes, hashing, and

key-exchange protocols. This section follows the outline and vague information provided by the older literature.

We explain post-quantum cryptosystems in section 3, which are new classical cryptosystems immune to quantum foes, their integration into existing blockchains, and implications infused by these cryptosystems on scalability and performance.

Hybrid quantum blockchains lay the trajectory toward the adaptation of fully quantum blockchains to be deployed over the quantum Internet. They propose blockchain schemes comprising both classical and quantum components: classical channels and quantum channels. QKD is the cornerstone of these mostly conceptual systems. A detailed description of the current state of fully quantum blockchain research is presented in section 4. These blockchain concepts are based entirely on quantum computing technologies with absolutely minimal classical components to sustain them.

The strengths, weaknesses, limitations, and gaps of the existing literature are discussed in section 5.

From a general perspective, section 6 sheds light on what could be done in the future in quantum and post-quantum blockchains.

2. Background Technology

This section aims to give a comprehensive understanding of preliminary technologies. In order to comprehend quantum blockchains and post-quantum blockchains, researchers need to have considerable insight into classical blockchains, classical cryptography, and quantum computing, and how quantum computers compromise classical cryptography. Additionally, it is essential to educate on how post-quantum and quantum blockchains may repel quantum threats.

2.1. Classical Blockchains

As Bhutta et al. [1] mention, a blockchain is a decentralized network that facilitates transactions/data without the presence of a central authoritative party, and this fact has fueled the popularity and adoption of this technology in the past 15 years. The immutability and security it provides rests on decentralized consensus protocols and classical cryptosystems. We will be exploring blockchain elements, i.e., how peers recognize one another for transactions (i.e., addresses), the structuring of the decentralized data (i.e., data structure), and the protocol for maintaining and agreeing on new

data entries (i.e., consensus mechanism). Bitcoin will be the basis for the

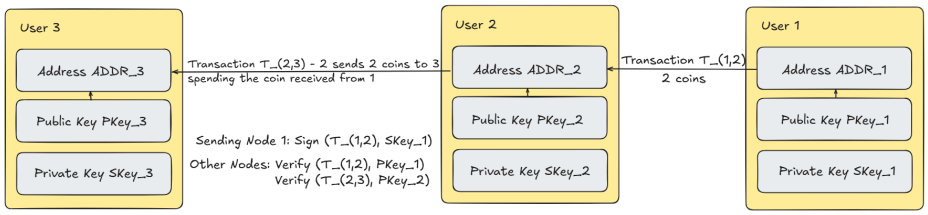

Figure 1: An illustration of blockchain structure

explanation. Beyond digital currency, blockchain has found its way into many application domains, but all implementations share the same concepts at the core, although many changes have been infused into the structure of blockchain over time.

Unique identifiers known as addresses for participants are generated using public key cryptosystems: RSA[2], Digital Signature Algorithm(DSA)[3], and Elliptic Curve Digital Signature Algorithm (ECDSA)[4]. Transactions are signed with private keys and verified using public keys. Blockchain user addresses, at times derived by hashing public keys, are usually generated per transaction or per a series of transactions to maintain privacy. To ensure immutability, transactions are stored in a sequence of blocks linked by hash pointers. Each block includes a header with metadata, including timestamps and nonces. Hash functions, such as SHA-2 and SHA-3, ensure data integrity and preimage resistance.[5] Mechanisms like Bitcoin's proof-of-work enable decentralized agreement. Miners solve computational challenges to add blocks, ensuring network security and incentivizing participation. There are three types of blockchains based on access (see Figure 2).[6] Private chains are restricted to a group, for instance, an organization, while public chains such as Bitcoin are open to anyone. Consortium blockchains are semi-decentralized blockchains, whereas hybrid chains are a combination of private and public.

A. Blockchain Address: Participants each need a unique address. This address is generated using the public key of the key pair generated by public key cryptography. These cryptosystems include RSA[2], DSA [3], and ECDSA [4]. Public keys are exchanged openly, while the private key must be kept in utter secrecy. A message can be signed with the private key, and other nodes can verify the authenticity of the signature utilizing the corresponding public key. There are standardized algorithms to derive an address

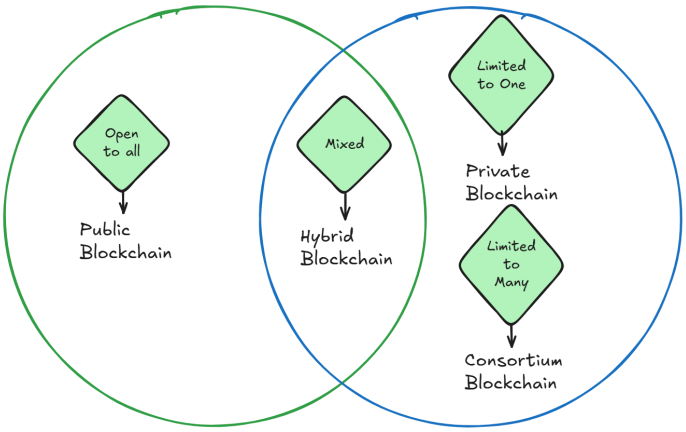

Figure 2: Types of blockchain based on access [6]

from a public key. Nodes instruct other nodes to send coins to their address, dispatch these coins subsequently using the same address, and use the private key to validate the transaction. And that expense is verified for authenticity using their public key (i.e, signature verification). According to Khalilov and Levi,[7] wallets usually generate/use multiple addresses to ensure anonymity.

B. Block Data: Transactions or other data are stored in homogeneous data structures called blocks, which are connected by hash pointers. Blocks have a set of transactions and a block header containing the hash of the previous block. If an adversary tampers with the data in a block, the hash links are broken, they would have to recalculate the hashes of all subsequent blocks which demands obscene amounts of computation, and add to that the decentralized nature and Proof of Work (PoW) consensus [8], this is impossible even for the most powerful supercomputers. Header metadata also includes a timestamp and a nonce. Hash functions from the SHA families are utilized to create the hash fingerprint for a block. [5] Hash functions are non-reversible (not possible to reverse-engineer), and the only way to find collisions with a classical computer is to brute force through the search space.

C. Consensus: To ensure security and reliability of the chain, it is essential for nodes to come to an agreement on the contents of new blocks. Miners compete in PoW to crack the hash puzzle to be able to create a block, and Bitcoin uses PoW consensus to select a miner to create a block of verified

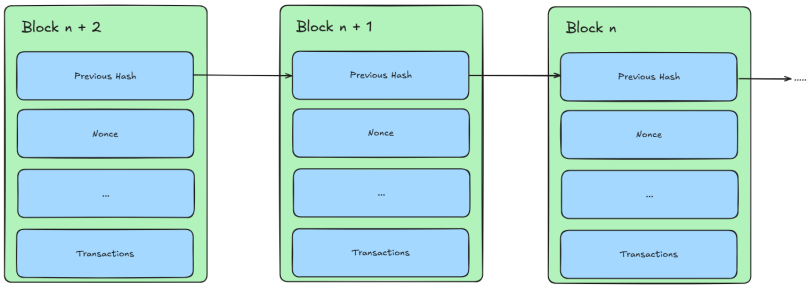

Figure 3: An illustration of blockchain structure.

transactions, and in turn, rewards them with coins. The puzzle involves finding a nonce that results in the block hash being within a predefined value. The first miner to obtain such a value broadcasts it over the network. When some node verifies this solution and the proposed block, it appends it to their chain. After a number of blocks, it becomes clear which block was adopted by the majority of the network, and therefore, the longest chain is established and accepted. Before finalizing a block, miners validate pending transactions from a pool. A double-spending attack requires an attacker to outpace the network in solving PoW, which is unlikely since the network's collective computational power exceeds that of a single attacker. However, if the attacker controls over 50% of the network's computational power, they could manipulate transaction validation, known as a 51% attack.[9]

D. Smart Contract: These are self-executing programs kept on blockchains. They have terms of agreements among parties written into them. They nullify the necessity for a trusted third party to instigate conditional services. When certain terms are met in the environment, certain routines execute in an "IF-ELSE" manner.[10] Smart contracts can be simple programs to dispatch cryptocurrency or decentralized applications running on the blockchain.

2.2. Quantum Computing

Richard Feynman introduced quantum information theory in his 1982 work.[11] Quantum computers operate on quantum physics. Qubits, represented by quantum particles, have two different states, such as electron spin (up and down).[12] They exhibit properties like superposition and entanglement. A qubit can be in a state between 0 and 1, known as superposition, both with probabilities assigned to them. According to Ronnow et al. [13],

this uncertainty, this ability to operate on many states simultaneously, can give exponential speed-ups over classical computing. Upon measurement, the superposition collapses to either 0 or 1, resulting in the loss of quantum information encoded in the probabilities. Uniform superposition suggests a state where both basis states are equally likely. These phenomena can extend to more than one qubit; for instance, 2-qubit systems have 4 basis states: 00, 01, 10, and 11. Qubits can become interdependent, and this is known as entanglement in space; temporal entanglement (i.e., entanglement in time) is a more complex, different phenomenon. This phenomenon can lead to the state of one particle influencing the state of another instantly. When one qubit collapses, the other collapses instantly. Quantum computers can operate on all 2^n states (i.e., coefficients).

The superposition of a qubit can be presented as a linear combination of states

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

The general state $|\psi\rangle$ can be expressed as:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

Upon measurement, the state always collapses to $|0\rangle$ or $|1\rangle$. For $|\psi\rangle$, probabilities of collapsing to 0 and 1 are $|\alpha|^2$ and $|\beta|^2$ respectively and $|\alpha|^2 + |\beta|^2 = 1$. [14] Quantum gates are operators that act on qubit registers. Examples are Hadamard; Pauli X, Y, Z; Controlled NOT (CNOT); etc. A pure qubit state can be represented as a point on the surface of the Bloch sphere, as shown in Figure 4. The general state of a qubit is given by:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle,$$

where $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi)$ are spherical coordinates. Here, θ defines the angle from the z-axis, and ϕ specifies the azimuthal angle in the x–y plane. This geometric interpretation provides an intuitive visualization of qubit superposition and relative phase.

There are early quantum algorithms that are useful not in the sense that they solve a concrete problem in computing, but in that they emphasize how quantum computers can be exponentially faster than their classical counterparts in certain domains. Deutsch-Jozsa algorithm [15] determines whether

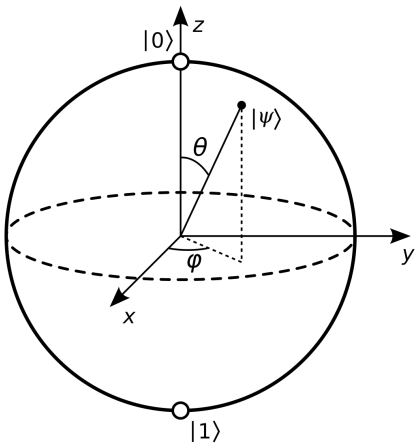

Figure 4: Representation of a pure qubit state as a point on the surface of the Bloch sphere

a given function is constant or balanced using only one evaluation, while a classical algorithm would require at least half of all possible function evaluations in the worst case. There is Simon's problem, which aims to find a bit string of order n. The classical approach takes $O(2^{n-1})$ queries, where Simon's algorithm [16] takes $O(n)$. The Bernstein-Vazirani problem [17] also involves finding a bit string where the classical approach is $O(n)$ but the quantum algorithm obtains the solution in a single run.

2.3. The Quantum Threat

The algorithms introduced so far, including useful algorithms such as Shor, form a framework known as the Hidden Subgroup Problem (HSP).[18] The problems they solve sit in between NP and NP-complete in a classical sense. As discussed, quantum computers offer exponential speedups for some computationally hard problems over classical computers, which, according to Leymann and Barzen[19], poses certain threats to some classical security mechanisms (see Figure 5). Many popular blockchains utilize elliptic curves for asymmetric cryptography (i.e., ECDSA) and SHA256 for hashing. The purposes of these hashes include address generation, block linking, transaction ID generation, etc. Shor's algorithm's ability to factor large integers and solve discrete logarithms, and hence derive private keys from public keys, and session keys in schemes such as RSA, ECDSA, and Diffie-Hellman key exchange (based on discrete logarithms) could break the Internet. If Grover's algorithm is further developed to efficiently invert hash

functions, PoW for consensus may become vulnerable, theoretically enabling the rewriting of the blockchain with a forged chain. Current quantum computers are not advanced enough to perform these efficiently, but they will be in the near future.[20]

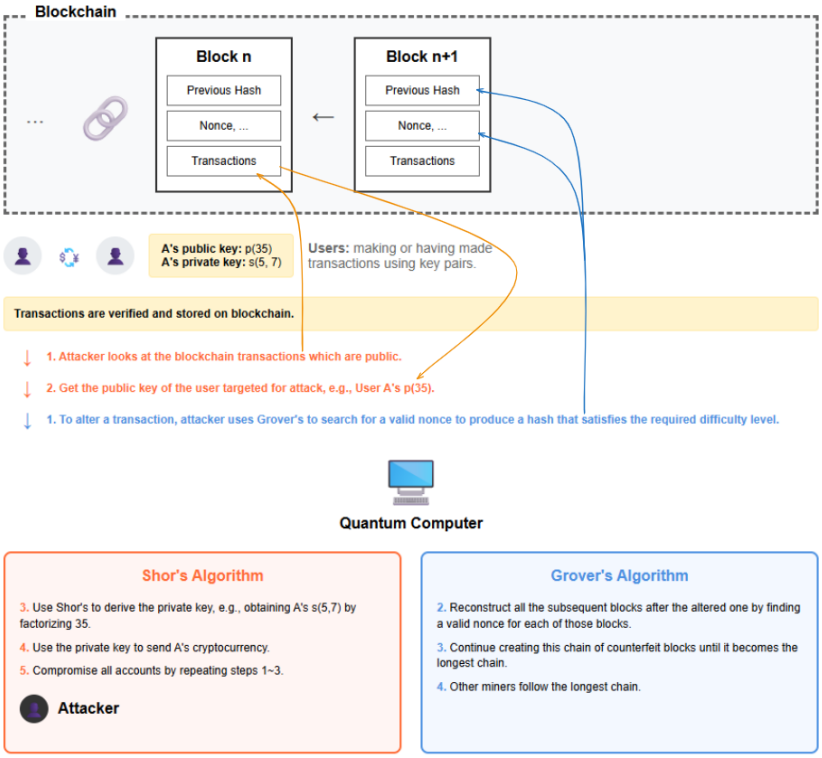

Figure 5: Quantum threats in Blockchain

A. Shor's Factorization: RSA relies on the factorization of large numbers, while DSA and ECDSA rely on discrete logarithms, both of which are efficiently solved on quantum computers. Blockchain nodes sign transactions with their private key, and other nodes can authenticate the transaction using the corresponding public key. If a quantum adversary derived the private key from a public key, they could impersonate the owner of the public key. Shor proved that his algorithm runs in polynomial time. [21] It can break RSA2048 in 10 minutes on a 10MHz quantum computer, while a 1THz classical computer would take 65 mil-

lion years. The frequency of the quantum computer is the microwave resonant frequency of the qubit.

B. Grover's Unordered Search: Instead of classical $O(N)$, Grover's algorithm can search through an unsorted space at $O(\sqrt{N})$. A practical implementation of Grover's algorithm could jeopardize all hash-related operations in a blockchain. Hashes are used for block validation, address generation, and hash pointers. Quantum miners would always find the winning nonce faster than classical miners. Therefore, they would dominate the block content and rewards. Also, being able to efficiently find hash collisions without having to brute force, quantum miners would be able to rewrite the blockchain with malicious blocks. This algorithm is based on the diffusion operator [22] — an operator that spreads probability over all measurable states in a multi-qubit system. Currently, there are no implementations of this for large problems. Unlike Shor's algorithm, popular blockchains are not particularly vulnerable to Grover's algorithm. PoW consensus like RandomX is immune to Grover's attacks.

2.3.1. Quantum Prime Factorization and Discrete Logarithm Solving Beyond Shor's Algorithm

Shor's attack is defined on universal quantum computers. Adiabatic Quantum Computing (AQC) has been utilized in factoring large integers into prime factors. This has been realized, in general, by solving optimization problems on D-Wave's quantum annealers. Jiang et al. [23] have described two methods to factor integers into primes via Quantum Annealing (QA) employing graph minor embedding to map problems to hardware: direct optimization and modified multiplication tables. Their method is resource efficient since they use $O(log^2 N)$ qubits, improving over prior methods. They have factored 15, 143, 59989, and 376289 on the D-Wave 2000Q annealer. Maezawa et al. [24] propose a quantum annealing machine designed specifically for prime factorization (PF), rather than performing prime factoring on commercial annealers, by inverting a QA-based Boolean multiplier circuit. They have introduced an Application-Specific Annealing Computing (ASAC) architecture to optimize hardware for factoring. They focus on hardware scalability and specialization, but do not demonstrate large-scale factoring. Want et al. [25] present a quantum annealing approach to prime factorization by optimizing the Ising model parameters for D-Wave Quantum Processing Units (QPU). The factorization is encoded into a Quadratic

Unconstrained Binary Optimization (QUBO) by using a multiplication table method. Their key innovation lies in significantly optimizing the local field parameters (h) and coupling (J) — reducing their ranges by 33% and 26% compared to previous work — which improves the stability of the qubit chain and allows larger factorizations. They successfully factored a 20-bit integer (i.e., 1,028,171) with just 88 qubits, surpassing previous quantum annealing records. Wronski [26] transforms the discrete logarithm problem (DLP) over prime fields into a QUBO problem solvable by quantum annealers. However, there is exponential growth in qubits, which limits scalability (e.g., 16-bit primes require 3,724 physical qubits). Mahasinghe and Jayasinghe [27] have formulated the DLP problem into a QUBO compatible with annealers. The DLP is first transformed into a pseudo-boolean optimization and then converted this into a QUBO using Rosenberg's quadratization to handle high-degree terms with auxiliary variables. This method faces scalability challenges due to exponential pre-computation and qubit constraints. In another work by Wronski et al. [28], the elliptic curve discrete logarithm problem (ECDLP) has been formulated into a QUBO to run on commercial annealers. The method is impractical for real-world parameters due to qubit demands (256-bit primes need 50 million qubits). The direct method requires $3n^3$ logical qubits for Edwards curves. Ding et al. [29] developed a novel approach to PF using QA by encoding a binary multiplier circuit into Pegasus of D-Wave's quantum processors. Encoding a controlled full-adder (CFA) into an 8-qubit block allowed them to construct large multipliers by replicating CFAs in a grid. They factored $8,219,999 = 32,749 \times 251$ — the largest number ever factorized on a quantum annealer without classical preprocessing — using techniques such as thermal relaxation and iterated reverse annealing.

It is evident that quantum annealing may be ahead of the universal quantum computers in dismantling classical cryptography by solving prime factorization and DLP, and hence, classical blockchain. On actual universal quantum hardware, no integer above 21 has been factored into primes via Shor's algorithm.[30]

2.4. Solutions to the Quantum Threat

Two main approaches have emerged in addressing quantum threats to blockchains. One is focused on substituting quantum-vulnerable components of classical blockchains with quantum-immune post-quantum classical components, i.e., post-quantum blockchains. The second one attempts to inte-

grate quantum algorithms, tools, quantum tech, and quantum phenomena into the implementation of blockchains, i.e., quantum blockchains. Post-quantum blockchain is based on post-quantum cryptography. These cryptosystems replace vulnerable cryptosystems like factoring-based ones (encryption, signature, and public key) with quantum-resistant components. These keys currently don't give small key, ciphertext, signature sizes, and low complexity altogether. Classes of such cryptosystems are Lattice-Based, Hash-Based, Code-Based, Multivariate-Based, and Super-Singular Elliptic Curve Isogeny. Quantum blockchains utilize QKD, Quantum Bit Commitment (QBC), Quantum Signature, and teleportation, among other quantum technologies. These blockchains are running on quantum networks/infrastructure, which are all part of the quantum Internet. Quantum teleportation enables the transmission of data in qubits between parties.

3. Post-Quantum Blockchains

3.1. Motivation for Post-Quantum Cryptography and Overview of Post-Quantum Blockchains

The advent of quantum computing has made it theoretically possible to factor large numbers and solve large discrete logarithmic problems compromising the security of classical public key cryptosystems: Shor [31] — can perform these in polynomial time with a sufficiently large quantum computer, and Grover [22] — quadratically speeds up the brute force hash collision search. This necessitates quantum-resistant cryptography. When it comes to blockchains that depend on cryptography, the most practical solution within the current infrastructure and technology is to replace cryptographic primitives such as signature schemes, encryption schemes, and hash functions with quantum-resistant counterparts cryptographic primitives. These schemes and blockchains, along with their underlying structure, would still be classical rather than quantum technologies, such as quantum blockchains and quantum networks.

3.2. Quantum Computing Threats to Blockchain

Threats to Consensus Mechanisms

PoW is the consensus of many popular public blockchains; this involves miners brute-forcing through a hash input space frantically to solve a cryptographic puzzle. A target hash with a fixed number of zeros for the block is the answer, and a nonce space is brute-forced through to find a suitable

nonce. A quantum miner finds the target nonce with a quadratic speedup. [32] This compromises the entire consensus reward mechanism by giving the quantum miner an unfair advantage. Then there is the 51% attack. [33] In a scenario with quantum computers, adversaries would not even need 51% of classical hashing power, given how much faster their nonce brute force is. This would result in double spending by including the same Unspent Transaction Output (UTXO) in two transactions and creating blocks with both of these transactions. The longest chain is king: it is accepted by all nodes eventually.[34]

Also, using Grover's algorithm, one can modify the local chain rapidly by faster calculation of all blocks' hashes from the mutated block, which would be accepted by the network as it becomes the longest, as described above in Bitcoin.

Quantum Signature Threats

These are quantum-resistant public key cryptosystems. Shor's algorithm on quantum computers can efficiently break RSA, ECDSA, and DSA signatures, as these schemes are dependent upon the difficulty of prime factoring and discrete logarithm problems. Using Shor's computation as described above, corresponding private keys would be derived from public keys. This would lead to forging valid signatures of nodes and signing transactions impersonating those nodes, where the adversary would spend those nodes' funds.

3.3. Post-Quantum Cryptographic Primitives

3.3.1. Post-Quantum Hashing

It is the general opinion of the community that current hashing is not nearly as threatened by quantum computing as public key cryptography. This is due to the fact that current hashing algorithms can be improved by increasing their output size, thereby mitigating the effect of the quadratic speedup afforded by Grover's algorithm. [22] Adding extensive quantum immunity, different quantum and post-quantum hash functions have been proposed. Zhou and Lu[35] propose a quantum hash function based on walks promising absolute security. This function bears resemblance to the hash function described by Lu et al.[36]. Hatanaka et al.[37] have presented a photonic hash function based on Gaussian Boson Sampling (GBS); note that this work is not peer-reviewed as of date. Zhou et al.[38] have described a more improved version extending on the work of Zhou and Lu[35]. This adds

parity dependence to their scheme. The primary focus of this section is to explore post-quantum signature and encryption schemes since those aspects make up what is immediately threatened by quantum computing.

3.3.2. Post-Quantum Public Key cryptosystems

This section explores different types of post-quantum signatures and encryption schemes (see Figure 6) and how they are applied to blockchains in various literature in recent years. The idea behind post-quantum cryptography is that they are based on the difficulty of mathematical problems that do not have a polynomial-time quantum algorithm. The National Institute of Standards and Technology (NIST) has standardized post-quantum cryptosystems. They also describe a list of characteristics for post-quantum cryptosystems for blockchains.

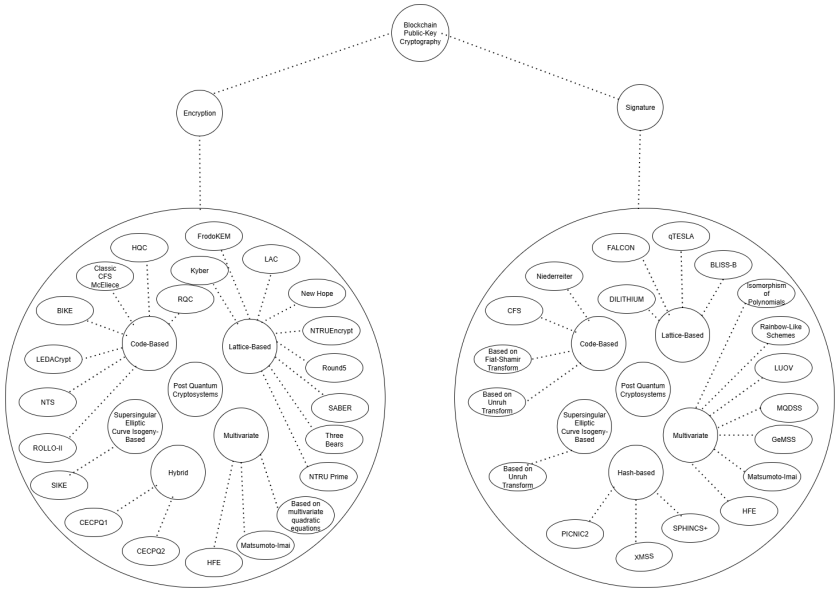

Figure 6: Post-quantum public key taxonomy

A. Lattice-Based Cryptography: Lattice-based is the most popular family of post-quantum cryptosystems. They are based on mathematical lattices: sets of unordered points in a finite-dimensional space. [19] Lattice-based cryptosystems depend on the hardness of lattice problems such as the Short Integer Problem, Closest Vector Problem, and

Shortest Independent Vector Problem. [19] Although these cryptosystems are relatively simple to implement and compute, and they are lightweight in the sense that their key, signature, and ciphertext sizes are relatively large, much like other post-quantum families, compared to their classical counterparts. Examples for lattice-based cryptosystems include Nth-degree Truncated Polynomial Ring Units (NTRU), KYBER, Guo-Lyubashevsky-Peikert (GLP), Dilithium, Ring Learning With Error (RING-LWE), and Fast Fourier Lattice-based Compact Signatures Over NTRU (FALCON). Most post-quantum cryptosystems, for instance, are based on polynomial algebra, Learning with Error (LWE), or variants like Ring-LWE problems [39].

Examples for lattice-based cryptosystems include XMSS, Lamport, SDS, W-OTS+, and SPHINCS+.

B. Code-Based Cryptography: Pratama and Krisna[40] have presented an extensive comparison between RSA and McEliece; McEliece is the most popular code-based signature scheme. [41] It's based on the syndrome decoding problem. Code-based cryptosystems are dependent on error-correction codes. McEliece is fast in execution but needs to store ginormous matrices as private and public keys; therefore, research needs to be done on matrix compression and restoration techniques. Different coding techniques for code-based cryptography are described by Lee et al.[42]. Other than McEliece, there are Niederreiter and Universal One-Way Hash Function (UOWHF). Key sizes and other parameters of code-based cryptosystems can be adjusted, resulting in different performance ratings and security levels. The code-based signature schemes ROLLO (Rank-Ouroboros, LAKE, and LOCKER) and Rank Quasi-Cyclic (RQC) both use 320-bit private keys, while the highest security Hamming Quasi-Cyclic (HQC) signature has private keys of over 15kb. On average, even with compression mechanisms, code-based schemes' keys are much larger than classical cryptosystems.

C. Super Singular Elliptic Curve Isogeny Cryptography (SIKE): These cryptosystems use the mathematical properties of supersingular elliptic curves and isogenies (special mappings between curves) to create secure cryptographic protocols. These systems rely on the difficulty of determining the isogeny between two elliptic curves, even when given partial information. SIKE offers compact key sizes and strong security

against both classical and quantum attacks, making it a prominent contender in post-quantum cryptography. Despite its promise, SIKE can be slower than other cryptosystems due to the complexity of its operations. These schemes are based on isogeny protocols on elliptic curves described by Rostovtsev and Stolbunov.[43] According to Microsoft [44], SIKEp434 is a good reference for SIKE key sizes. Biasse et al.[45] and De Feo et al.[46] give widely approved SIKE schemes. Examples for this family include Supersingular Isogeny Diffie-Hellman (SIDH) and Commutative SIDH (CSIDH).

D. Multivariate-Based Cryptography: These cryptosystems are based on the difficulty in solving systems of multivariate equations.[47] The most renowned examples for these cryptosystems are based on the use of square matrices, Hidden Field Equations, and random quadratic polynomials. These signatures are quantum-resistant but have large keys and ciphertexts. Unbalanced Oil and Vinegar (UOV) is another example.

E. Hash-Based Cryptography: The birth of this family was marked by Lamport's proposal of a signature scheme based on a one-way function. The security of the underlying hash function determines the security of these schemes. Extended Merkle Signature Scheme - Extended Merkle Tree - (XMSS) [48], and SPHINCS [49] are popular examples among others, like their variants and Stateless Digital Signature (SDS), Winternitz One-Time Signature (W-OTS). Alternatives have been presented. Another is that XMSS is being given a single authentication path instead of a tree. [50] This approach reduces possibilities for user tracking and amplifies anonymity.

F. Hybrid Cryptography: Certain post-quantum cryptosystems have been cracked by classical algorithms. Castryck and Decru[51] cracked SIDH (Singular Isogeny Diffie-Hellman). They broke the SIKE algorithm that reached the fourth round of NIST using a classical magma implementation. These incidents inspired hybrid cryptosystems that combine classical and quantum cryptographic primitives. The expectation is that in a classical attack, classical cryptography would protect data, whereas in a quantum attack, the post-quantum scheme would provide protection. Google experimented with a hybrid scheme that combines

an ECC-Diffie-Hellman scheme with New Hope. [52] Hybrid cryptosystems involve implementing two complex cryptosystems, resulting in massive computational and communication overhead.

3.3.3. Post-Quantum Cryptosystems Implementation into Blockchains

This section will discuss how researchers have integrated post-quantum cryptosystems into blockchains. A proper entry point for this endeavor is the work by Lone and Naaz.[53] They have described classical cryptography in the context of Bitcoin and Ethereum, concluding with the quantum threat and an introduction to post-quantum blockchain. It would be sensible to divide this section into post-quantum blockchain signatures; smart contracts and decentralized applications; and post-quantum wallets.

Post-Quantum Signatures in Blockchain. The general idea is to take a blockchain application as it is and replace its signature scheme with a scheme accepted by NIST's current post-quantum standards. Anhao[54] has proposed a hash-based post-quantum bitcoin implementation. He has integrated XMSS as the signature scheme, and he believes it would lead to a hard fork in the blockchain. The abelian whitepaper [55] has introduced a lattice-based signature cryptocurrency with adjustable privacy. Their cryptoprimitives are based on the Shortest Integer Solution (SIS) and LWE problems. Those two were industry ventures into post-quantum blockchains, but that will stop at this point since our focus is on literature in academia. Scholars tend to lean toward hash-based and lattice-based approaches since they are mathematical and therefore flexible.

WOTS-S, which is a variant of hash-based WOTS with shorter keys and ciphertext, has been proposed by Shahid et al.[56]. They say signatures are much shorter than IOTA and SDS. The authors claim this is because they have used collision-resistant hashing for compression, unlike rivals that utilize bitmasks. Chalkias et al.[50] proposed an XMSS signature scheme named Blockchained Post-Quantum Signatures(BPQS). Unlike many hash-based blockchain signature schemes, this scheme can use the same key for several transactions at random or optionally, generate keys per transaction; in either way, it remains among the most computationally efficient. There is a lattice signature scheme proposed by Li et al.[57] where they have used random and different keys for different transactions. This key generation is related to wallets, which will be discussed later. Gao et al.[58] contributed to another work, this time, a post-quantum cryptocurrency. They have put

together a lattice-based delegation algorithm to randomly generate keys and sign by the preimage sampling algorithm. The signature is a double signature based on the SIS problem. Other than this signature scheme, the protocol is much like existing blockchains, i.e., it has address generation via public keys, consensus, and checking for double-spends, etc. Saha et al.[59] have presented a blockchain with lattice-based polynomial ring Identity-Based Encryption (IBE) scheme and aggregate signature along with certificate-less IBE to solve the key escrow problem. Li et al.[60] introduce an anti-quantum proxy blind signature scheme for blockchain, based on lattice cryptography, which can provide user anonymity and untraceability in the DApps of Blockchain IoT. Chao-Yang et al.[61] also presented a lattice-based blockchain signature scheme in which key pairs are generated with Bonsai Tree and RandBasis (Random Basis). Torres et al.[62] have constructed a Lattice-based one-time Linkable Ring Signature (L2RS), which they have used on a blockchain to create a new cryptocurrency. Linde[63] has constructed a post-quantum signature scheme for blockchain technology by combining a hash-based one-time signature scheme with Naor-Yung chaining.

Post-Quantum Wallets. To reduce key sizes and the number of key pairs that need to be stored, lightweight wallet components are essential. The lattice signature-based blockchain proposed by Li et al.[57] has a lightweight wallet that utilizes bonsai trees to generate keys. There is a root key which is the only key to be stored. For each transaction, the RandBasis algorithm creates a random Bonsai tree from this root, thereby preserving pseudo-random anonymity. An anti-quantum transaction authentication system for blockchain is given by Yin et al.[64], where they also have described a lattice-based authentication based on a root key and a bonsai tree, which expands a lattice space to a multitude of lattice spaces to get randomness and anonymity. In classical cryptocurrency, since key sizes were minimal, even storing all the keys from the past was not a cause for wallet bloat; therefore was not a principal concern, but post-quantum keys are generally much bigger, so researchers are attempting to store as few keys as possible and reduce key sizes.

Post-Quantum Smart Contracts and Decentralized Applications(DApps). Smart contracts and DApps, which are advanced smart contracts that execute as fledged applications, execute on the blockchains. Considering the stark differences between classical blockchains and post-quantum blockchains, experts

have been researching on applications and domain-specific programs that need to run on post-quantum blockchains since their underlying implementation needs to be different from their classical counterparts as well. Zheng[65] has proposed a complete smart contract process on post-quantum blockchain. He has named it BSCTQCAT (blockchain smart contract technique based on resistance to quantum computing attacks).

> The technique employs a digital signature algorithm based on a lattice cipher to enhance the resistance against quantum search attacks. By introducing the lattice cipher, more robust cryptographic protection is provided to ensure data security. Meanwhile, a smart contract authentication scheme is constructed to organize nodes on multiple heterogeneous chains by establishing a P2P network with an identity agent layer. According to the transactions on the chain, a trusted identity management and message authentication mechanism is established, enabling reliable communication between different chains. With this technique, the compartmentalization problem between different chains in the blockchain ecosystem can be effectively solved, and more secure and reliable blockchain smart contract services can be provided. [65]

IoT has been quite the topic in smart contracts and DApps in the recent five years. There is an attempt to merge post-quantum blockchain with SIoT (Social Internet of Things). [66] In his proposal, a multivariate ring signature protocol is presented: ring signatures create a combination of signatures and public keys of a set of other nodes (ring), which results in the validator not knowing which exact one in the group has signed. Gao et al.[67] describe a post-quantum blockchain-powered voting application that is powered by Niederreiter's code-based cryptography with a certificate-less, traceable ring signature. They put great emphasis on auditing, accounting for both malicious attacks and voting mishandling. This scheme has the ability to audit voters operating incorrectly and resist quantum attacks by adopting certificate-less and code-based cryptography. Yu and Hui[68] proposed a NTRU lattice-based certificate-less signature blockchain voting application.

3.3.4. Post-Quantum Consensus and Privacy

Classical Consensus. The most popular consensus algorithm is Bitcoin's PoW. [34] Consensus algorithms can be classified into 2 families: proof-based and

voting-based. Proof-based consensus is common in public chains, whereas voting-based is popular in private blockchains. Jose and Panchami[6] provide a list of common classical consensus protocols and the byzantine generals problem, which can approximate the consensus problem in blockchains where there is trustless decentralization and malicious/erroneous nodes. The purpose of a consensus algorithm is to bring all nodes to agreement on the update (new block) a node (miner) is about to make. As Jose and Panchami[6] note, distributed ledgers lack a trusted central authenticator, which necessitates consensus mechanisms. Therefore, the consensus mechanism is implemented to prevent attacks like double-spending, ensure fairness and security, mitigate malicious/erroneous behaviour of nodes, etc. Consensus algorithms decide which node gets to update the chain and which data inside the new block is valid.

Post-Quantum Consensus. Yi et al.[69] have presented a consensus algorithm that leverages a post-quantum threshold signature scheme based on solving quadratic equations in a finite field, ensuring resistance to both quantum and classical attacks. Unlike classical consensus such as PoW and Practical Byzantine Fault Tolerance (PBFT), this approach requires more than half the nodes to sign the new block using the threshold signature, improving efficiency and security for future quantum-resistant applications. Kim et al.[70] have described an efficient blockchain with a new post-quantum consensus mechanism. The signature scheme is FALCON. Transactions per Second (TPS) is usually lessened by post-quantum signature protocol, but they have claimed the consensus protocol — post-quantum delegated proof of luck (PoL) — compensates. In this PoL combined with a delegated approach, they have eliminated the dependency of PoL on trusted execution environments (TEE) and utilized verifiable random functions (VRF) for fairness and randomness. It is also less prone to centralization than PoW, Proof of Stake (PoS), and Delegated PoS. Ding[71] has proposed a consensus based on multivariate quadratic equations over GF(2). The NP hard problem is the Multivariate Quadratic (MQ) problem. The algorithm constructs polynomials using hash values, assigning them as coefficients. Miners solve these equations to find a vector that satisfies the system, ensuring security against quantum attacks. There is a modified PoW consensus algorithm from Chen et al.[72] that is not described at a lower level but seems promising. It has a dynamic Difficulty Adjustment Algorithm (DAA) to adjust the difficulty of the problem for the current block. Unlike Bitcoin's PoW, this utilizes the

problem of solving multivariate quadratic equations, which is NP-hard, for the consensus problem, instead of the SHA256 hash puzzle. The old PoW is vulnerable to Grover's quantum attack because of SHA256. The miner's work includes both computational and storage capabilities.[72]

3.3.5. NIST standardization and insights

The National Institute of Standards and Technology (NIST)[3] presented an enhanced version of the DSA public key encryption scheme. The NIST post-quantum cryptography standardization aims to encourage the development of cryptographic algorithms that resist quantum attacks and certify them. With quantum computing breaking current cryptographic systems like RSA and ECC, NIST initiated a multi-phase process to evaluate and standardize new quantum-resistant cryptosystems (signature/public key encryption). This effort is crucial to secure digital communications, blockchain systems, and other technologies vulnerable to quantum threats. The first round saw the passing of the following signature schemes (Table 1).[73]

Table 1: Round 1 results

Lattice-Based	**Code-Based**	**MPC-in-the-Head**	**Isogeny-Based**	**Multivariate**	**Symmetric-Based**
Hawk	CROSS	Mirath	SQIsign	UOV	FAEST
	LESS	MQOM		MAYO	
		PERK		QR-UOV	
		RYDE		SNOVA	
		SDITH			

MQOM	Multivariate Quadratic Optimization Method
PERK	Post-Quantum Encryption with Rank-based Keys
RYDE	Rank-based Yielding Digital Encryption
SDITH	Syndrome Decoding in the Hamming metric
QR-UOV	Quasi-Random Unbalanced Oil and Vinegar
SNOVA	Supersingular NOVA (isogeny-based scheme)
FAEST	Fast Authenticated Encryption with Short Tags
CROSS	Code-based Random Oblivious Signature Scheme
LESS	Lattice-based Encryption and Signature Scheme
Mirath	A post-quantum cryptographic scheme

SQIsign	Supersingular Quaternion Isogeny Signature
MAYO	A post-quantum cryptographic scheme

The third round Crystals-Kyber was selected as the Key Encapsulation Scheme (KEM) for standardization, and BIKE, Classic McEliece, Low-Quality Channel (LQC), and SIKE were advanced to the fourth round. [74] Among signature schemes, Crystals-Dilithium, FALCON, SCHINCS+ were selected for standardization. Fernández-Caramés and Fraga-Lamas[75] have presented extensive comparisons of KEMs and signature schemes applicable to blockchain that reached the second round in terms of key and ciphertext sizes, and they provide detailed performance comparisons of all these families, such as lattice, code-based, etc. Gheorghiu et al.[76] analyze the performance of post-quantum signature schemes.

3.3.6. Distribution of literature

Figure 7 presents the global distribution of literature related to post-quantum blockchain technologies and the foundational technological components that we have described in section 2. The geographic clustering visible in the map highlights the dominant research activity in regions such as North America and parts of East Asia. This distribution underscores the geopolitical and institutional landscape shaping current advances in post-quantum cryptography and quantum-secure distributed ledger protocols.

4. Quantum Blockchains

This section is concerned with the academic state-of-the-art of the integration of quantum technologies into blockchains and/ or the implementation of blockchain concepts on quantum technologies such as quantum cryptography, the most developed among which is QKD, quantum teleportation, QBC, entanglement based chains, Quantum Secure Direct Communication (QSDC), quantum signatures, etc. The composition of this section will be as follows: A brief review on quantum cryptography, quantum consensus in recent literature, and implementations of quantum blockchains in academia. In our view, quantum blockchain technologies are of four types: hybrid quantum blockchains, fully quantum blockchains (quantum signature), fully quantum blockchains (QKD-based), and decentralized applications on blockchain. The main emphasis is on quantum blockchain implementation rather than supporting technology such as quantum cryptography.

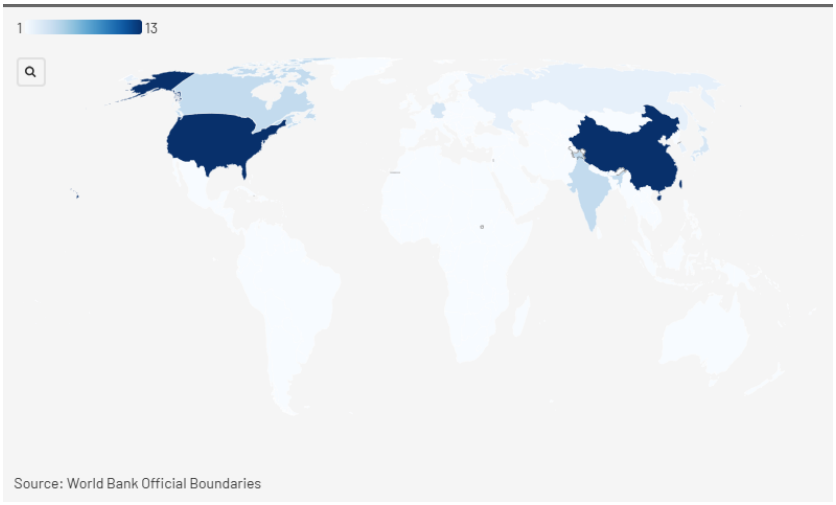

Figure 7: Global distribution of literature on post-quantum blockchain and background technologies

4.1. Quantum Cryptography

4.1.1. Quantum Key Distribution

This is the most developed family of quantum cryptographic primitives. Stephen Wiesner introduced "Quantum Cryptography" in the 70s at Columbia, New York.[77] Bennett and Brassard[78] then introduced QKD. This technology has been well developed compared to other quantum technologies, having been used to distribute keys over large distances, even utilizing satellites.[79] The following is a description of the BB84 QKD protocol by Bennett and Brassard[78], and other schemes that came after.

BB84. Quantum key distribution's (quantum cryptography's in general) absolute (unconditional) security is guaranteed by the laws of quantum physics.[78] One such is Heisenberg's uncertainty principle, which states that it is impossible to measure two physical properties of a particle. The second is the photon polarization theorem that makes it impossible to clone quantum systems. These laws ensure that the eavesdropper who tampers with the message by intercepting, i.e., measures the state of the transmitted quantum system — collapses the system and is unable to recreate it, which in turn, results in the discovery of his attacks.[80]

1. Alice encodes each bit onto a photon using one of two orthogonal bases (Figure 8):

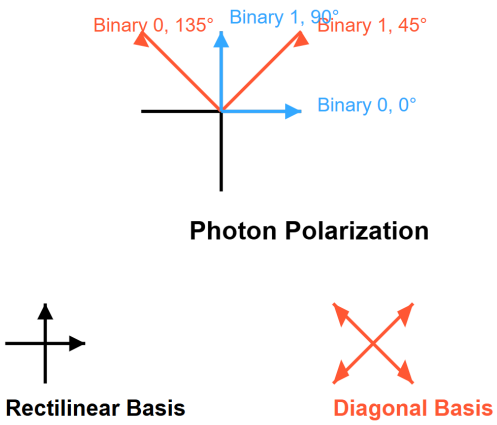

Figure 8: Rectilinear and diagonal basis

- Rectilinear basis: $|0\rangle$ (horizontal) and $|1\rangle$ (vertical)
- Diagonal basis: $|+\rangle$ (45°) and $|-\rangle$ (135°)

2. Alice sends the photons to Bob, who randomly chooses a basis (rectilinear or diagonal) to measure each photon.

3. After transmission, Alice and Bob publicly compare their chosen bases and discard bits where their bases did not match.

4. A subset of the remaining bits is used for error checking to detect eavesdropping, as an interceptor (Eve) would introduce disturbances due to the no-cloning theorem.

5. If the error rate is acceptably low, the remaining bits form a secure cryptographic key.

B92. B92 is a modified version of the BB84 protocol that utilizes only two states instead of four. In this scheme, a photon polarized at 0° in the rectilinear basis represents a binary 0, while a photon polarized at 45° in the diagonal basis represents a binary 1. [81]

There are other technologies that implemented QKD. They are either improved variants of it or entire network infrastructures based on it. Six-State Protocol (SSP), SARG04, Einstein-Podolsky-Rosen (EPR), and AK15 are

some of the improved versions. The Secure Communication based on Quantum Cryptography (SECOQC) QKD Network and the Defense Advanced Research Projects Agency (DARPA) are among such networks.

4.1.2. Quantum Signatures

QKD is a symmetric cryptosystem: a one-time pad is shared between a couple of nodes via a secure quantum channel, and this is used for symmetric encrypted communication over an unsecured channel.[80] But classical cryptography is asymmetric. Therefore, an equivalent signature paradigm on quantum mechanics was necessary to implement public key cryptography on blockchain.

Wang and Yu[82]: A quantum signature based on quantum state computational distinguishability with a fully flipped permutation (QSCDff) problem. The quantum informational security of this protocol relies on the QSCDff problem. The solution is to distinquish between a couple of quantum states for some random

$$\pi \in \kappa_n = \left\{ \pi \in S_n \mid \pi^2 = \mathrm{id},\ \forall i \in \{1, 2, \ldots, n\} \right\}.$$

These states are

$$\rho^+_{\pi(n)} = \frac{2n!}{1} \sum_{\sigma \in S_n} (|\sigma\rangle + |\sigma\pi\rangle)(\langle\sigma| + \langle\sigma\pi|)$$

$$\rho^-_{\pi(n)} = \frac{1}{2n!} \sum_{\sigma \in S_n} (|\sigma\rangle - |\sigma\pi\rangle)(\langle\sigma| - \langle\sigma\pi|).$$

It has been proven that if $\pi \in \kappa_n$ is random and unknown, there is no quantum algorithm that can solve the QSCDff problem with non-negligible advantage. However, this problem can be quickly solved with the solution of π, so that π would serve as a trapdoor in the quantum signatures. They have tested a gate model circuit to distinguish between these states, to generate $\rho^+_{\pi(n)}$ and to perform conversion from $\rho^+_{\pi(n)}$ to $\rho^-_{\pi(n)}$, which is given by the following operation:

$$\frac{1}{\sqrt{2}} (|\sigma\rangle + |\sigma_\pi\rangle) \rightarrow \frac{1}{\sqrt{2}} \left((-1)^{\mathrm{sgn}(\sigma)} |\sigma\rangle + (-1)^{\mathrm{sgn}(\sigma_\pi)} |\sigma_\pi\rangle \right)$$

The signer performs the $\rho^+_\pi(n)$ generation algorithm to obtain the public key $|PK\rangle = \bigotimes_{i=1}^n \rho^{i+}_\pi$. The signer has a key pair $(|PK\rangle, \pi)$. The signing process involves setting up decoy particles to detect eavesdropping. Verification

of the signature by witnesses involves setting up decoy quantum particles and a process involving two verifiers: they cannot self-verify.

Yang et al.[83]: Quantum public-key cryptosystems based on induced trapdoor one-way transformations; Liang and Yang[84]: Public-key encryption and authentication of quantum information. Yang et al.[14] have utilized both these schemes, which share many similarities and combine features from each. Both are based on Quantum One Way Trapdoor Functions (OWQT) as shown in Figure 9.

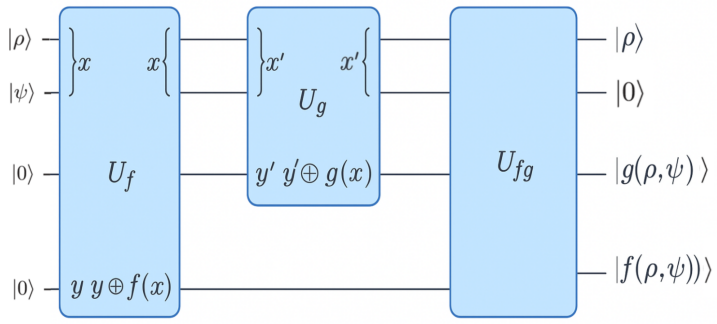

Figure 9: General quantum circuit for a trapdoor OWQT. [14]

Yang et al.[83] define the trapdoor OWQT as:

$$\text{UOWQT}\left(|\rho\rangle|\psi\rangle|0\rangle|0\rangle\right) = |\rho\rangle|0\rangle\, g(\psi,\rho)\, f(\psi,\rho)$$

where f and g constitute the trapdoor function $h(\psi, p)$ that is easy to operate, hard to invert, and easy to invert with trapdoor (secret s). f and g trapdoors are represented by their corresponding oracles. f and g will be the public key where the secret s be the private key. Alice encrypts state $|\psi\rangle$ producing the ciphertext:

$$|\rho\rangle|0\rangle\, g(\psi,\rho)\, f(\psi,\rho).$$

The decryption process of a verifier is:

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

The signed message is invalid after the quantum message is extracted. Therefore, this kind of signature can only be validated once. Nonetheless, it is possible to obtain a local copy of the signed quantum state.

Gottesman and Chuang[85]: Quantum Digital Signatures. Sending an m-bit message in this scheme uses up O(m) quantum bits for each recipient of the public key. This scheme shows some resemblance to Lamport's classical signature scheme, i.e., for instance, both use a series of private keys to sign a single message. Any digital signature scheme depends on a one-way function, where in this case, there is a quantum one-way function:

$$k \mapsto |f_k\rangle \quad \text{(easy)}$$
$$|f_k\rangle \mapsto k \quad \text{(impossible)}$$

where k is the private key (a bit string) and $|f_k\rangle$ be a corrresponding public key. By Holevo's theorem and the probabilistic nature of quantum state measurements, a measurement would reveal n bits of information about k for this is an n qubit state. Where the length of k is L and T copies are distributed, and $L - nT \gg 1$, the probability of obtaining k remains small. Given two signatures $|f_k\rangle$ and $|f_{k'}\rangle$, recipients can perform swap tests to determine if $k = k'$ although this is probabilistic. Given a signature $|\psi\rangle$ and k to verify $|\psi\rangle = |f_k\rangle$, perform $|k\rangle|0\rangle \mapsto |k\rangle|f_k\rangle$ and measure the second register. In a naive approach to fit the one way function into Lamport's signature, Alice selects k_0 and k_1 as private keys and announces $(0, |f(k_0)\rangle)$ and $(1, |f(k_1)\rangle)$ as public keys. To sign b, she provides (b, k_b). Bob verifies by checking if $|k_b\rangle|f(k_b)\rangle$ maps back to $|k_b\rangle|0\rangle$. They have concluded that a trusted key distribution centre would be most practical rather than P2P key distribution. Any signed message will be determined acceptable and transferable, acceptable but not transferable, or rejected. The scheme is secure against Alice's attempts to repudiate the message. That is, for any pair of recipients, with high probability, if the first recipient reaches the conclusion that the message is valid, then the second recipient reaches the message is valid. It is also secure against forging, that is, given access to a valid signed message $(b, s(b))$ and all available copies of the public keys, no forger has an appreciable chance of creating a message, signature pair $(b\prime, s\prime)$ (with $b\prime \neq b$) such that an honest recipient will accept it. They have provided those proofs in addition to generalizations and extensions such as multi-bit signing and symmetric swap tests among recipients.

Alharby et al.[86]: A Blockchain Smart Contract Based on Light-Weighted Quantum Blind Signature. A QKD protocol based on entanglement for a single-person signature is first described. The signature is a quantum state

whose time evolution is given by Schrodinger's equation:

$$i\frac{\partial\psi}{\partial t} = \hat{H}\psi.$$

The quantum blind signature system can prepare a general state of n qubits:

$$|\psi\rangle = \sum_{i=0}^{2^n-1} c_i|i\rangle.$$

The trader and the block creator establish a key using the BB84[78] protocol. This is applicable since the signature is blind. The trader sends the transaction message to the block creator via the classic channel, where the transaction message is signed by the sender by negotiated quantum keys and then attached to the block. The unitary operations before the comparison, after measurement of entangled bits, and decryption of the signature are shown in Figure 10.

Trader's signature	Particle b_i	Recovery operation of block creator
$\|\varphi_{a,R_i}^{+}\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$	$\hat{\sigma}_3$
$\|\varphi_{a,R_i}^{-}\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$	I
$\|\varphi_{a,R_i}^{\rightarrow}\rangle$	$\alpha\|1\rangle - \beta\|0\rangle$	$\hat{\sigma}_3\hat{\sigma}_1$
$\|\varphi_{a,R_i}^{\uparrow}\rangle$	$\alpha\|1\rangle + \beta\|0\rangle$	$\hat{\sigma}_3$

Figure 10: Unitary operations for signature [86]

After key distribution comes the creation of entanglement pairs by the block creator. The signature is a multipartite quantum state where each particle in the signature is a quantum state R_i.

$$|R_i(a)\rangle = |R_i(b)\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$$

where $|\alpha_i|^2 + |\beta_i|^2 = 1$ and $i = 1, 2, 3, \ldots, n$.

α_i and β_i represent the gradient values of the i-th pair of entangled particles and are owned by the business trader. The block creator uses the shared quantum key to decrypt and verify the signature. The blind removal transformation will be performed to obtain the transaction message.

4.1.3. Quantum Teleportation

Recall that quantum entanglement is a property that is essential for quantum information transfer; it is possible to quantify how entangled two qubits are, using standard entanglement measures. The four maximally entangled states made by two qubits are known as Bell states, and it is easily shown that these states cannot be stated as products of single qubit states. Also, these states make a basis for the space made by two qubits, known as the Bell basis $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ where,

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

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

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

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{4}$$

Suppose Alice wishes to send Bob two-bit classical information. Superdense coding is a way of achieving this task over a quantum channel, requiring only that Alice sends one qubit to Bob. A third party makes the Bell state $|\Phi^+\rangle$ and sends 1st qubit to Alice and the 2nd to Bob. Alice applies a quantum gate from a set of gates to her qubit, depending on what she wants to send, and then shares her (one) qubit with Bob. The resulting state can be determined based on what Alice wishes to send to Bob. Then Bob measures his qubit with respect to the Bell basis and receives the (2-bit) information Alice wanted to send him.

While superdense coding transmits two classical bits, teleportation realizes the transmittance of a quantum state $|\psi\rangle$. From Bennett et al.[87], the following can be formulated. The receiver shares a qubit from the Bell state $|\phi^+\rangle$ with the sender. The sender applies CNOT to their state $|\psi\rangle$ and their qubit of the Bell pair. Then Hadamard is applied to $|\psi\rangle$ qubit. Then he measures both these qubits in computational basis and sends the outcome to the receiver who, based on that, applies Z and X to their qubit to obtain the sent state $|\psi\rangle$. It is noteworthy that, although the second qubit's state collapses immediately upon measurement of the first qubit, it does not enable instantaneous communication. To obtain the quantum bit in transit, using the measured qubit of the entangled qubit, the receiver still has to

perform the computation necessary to construct the sender's qubit's state. Besides, the sender needs to transmit the outcome of their measurement to the receiver via a classical communication channel. Alice wants to teleport a qubit state to Bob. They share an entangled qubit pair, with each holding one qubit. Alice performs a Bell state measurement (BSM) on her qubit (her half of the entangled pair), collapsing the system into one of four possible states with equal probability. She then sends the result to Bob on a classical channel. On this information, Bob applies the necessary gates to his qubit, reconstructing the original state. Due to the measurement and no-cloning, Alice's qubit is destroyed in the process.[87]

4.1.4. Quantum Bit Commitment

Bit commitment is used in a variety of cryptographic elements: Zero Knowledge Proof, Multiparty Secure Transmission, and Oblivious Transmission. It involves two phases: Commitment and Announcement. In commitment, Alice chooses a bit and commits it to Bob. That is, Bob cannot determine the committed bit without more information. In the announcement, Alice reveals more information, and Bob can obtain the committed bit.[88] If Alice cheats, she changes the bit after commitment. Bob would cheat by discovering the bit before the announcement. A Bit Commitment (BC) protocol has two properties: concealing — Bob cannot cheat, and binding — Alice cannot cheat. Bennett and Brassard[78] introduced the first QBC. A QBC protocol is unconditionally secure if any cheating can be detected with a probability arbitrarily close to 1. But unconditionally secure QBC is not achievable according to the MLC no-go theorem.[89] Therefore, other families such as Cheat-Sensitive Quantum Bit Commitment (CSQBC) and Relativistic Quantum Bit Commitment (RQBC) have been developed. CSQBC is secure in the sense that it only needs to detect cheating with negligible probability, where punishment can be enforced. There have been a few works on CSQBC and RBC.[89] Hardy and Kent [90] and Sung and Wang[91] have proposed CSQBC protocols.

4.2. Blockchain Implementations on Quantum Technology

Over the last couple of decades, there have been many works on integrating quantum technology into blockchain, some even modeling the chain itself on qubits. This section will explore their breadth and depth.

4.2.1. Hybrid Quantum Blockchain (QKD-based)

Similar to the work by Kiktenko et al.[5], the quantum technologies in hybrid quantum blockchains are based primarily on QKD. Hence, they are mostly symmetric in terms of keys and encryption.

This overview will be useful in comprehending the literature next.

Before block production, these network nodes would authenticate themselves mutually, that is, every pair would establish keys with QKD. Mostly, in the block production phase, consensus and hashing could take an entirely classical form or might be based on quantum state transmission. That is, a hybrid quantum blockchain is one that primarily uses QKD for authentication, and utilizes a classical system for at least a part of its core functionalities: block production, consensus.

Kiktenko et al.[5]: Quantum Secured Blockchain. Apparently, it is an implicit convention in the community to begin any review on hybrid quantum blockchain with Kiktenko et al.[5]. They have utilized a QKD scheme for transaction authentication. That layer constructs symmetric keys pairwise. The blockchain itself has two phases: the creation of transactions and the construction of blocks that aggregate new transactions. A sender constructs the transaction similarly to a Bitcoin transaction with information about the sender, receiver, time of creation, amount to be transferred, and a list of reference transactions. This is sent to all other nodes. They verify it for fund sufficiency before aggregation onto a block. Broadcast protocol is used for consensus. Periodically, consensus is initiated where each node adds time-sorted and verified yet unconfirmed transactions to a new block in the local chain, ensuring all nodes create the same block and the same chain, i.e., avoiding forks. This offers high initial tolerance to dishonest/faulty nodes. This chain would repel Grover's attacks by increasing the hash size. They tested the proposal with a four-node, six-link network that consisted of an urban fiber QKD network.

Sun et al.[89]: Quantum-enhanced Logic-based Blockchain I: Quantum Honest-success Byzantine Agreement and Qulogicoin. This is a versatile quantum blockchain that is a general permissioned blockchain while also geared toward a cryptocurrency: "Qulogicoin." It is built on Kiktenko et al.[5], adding extensive improvements. They have incorporated quantum certificates and quantum protection into the syntax of transactions. The classical Byzantine fault tolerance of Kiktenko et al.[5] has been replaced by a new consensus:

Quantum Honest Byzantine agreement (QHBA). Also, a use case of this blockchain is presented where a punishment rule is formulated for CSQBC. QKD is utilized at the deployment level to establish mutual keys for every pair.

$$T_x = (x, y_1, \ldots, y_n, j; \alpha, \phi; \beta_1, \psi_1, \ldots, \beta_n, \psi_n)$$

Transaction syntax is as above, where it includes classical and quantum certificates, and Toeplitz' keyed hashing is used for transaction hashing. All miners validate the transaction for authenticity, including the hash validity and whether reference transactions are being double-spent, etc. After QHBA, a block is created with the transaction. This QHBA relies heavily on QSDC (Quantum Secure Direct Communication) and a quantum version of Shamir's three-pass protocol. The application in CSQBC has penalized cheaters by seizing some UTXOs (Unspent Transaction Outputs).

Sun et al.[92]: Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic. This adopts a vote-based consensus and a QKD-powered signature scheme. This signature scheme is unconditionally secure as claimed by them, and the work includes a logic-based scripting language for the creation of smart contracts and a quantum-resistant lottery protocol. This Unconditionally Secure Signature (USS) is built on Toeplitz' Hash Message Authentication Code (Hash MAC). They have named their signature Toeplitz Group Signature (TGS), which combines the Toeplitz hash MAC with a USS from some other work. Toeplitz keys are agreed on via a QKD network. According to them, this signature exhibits non-repudiation, transferability, and unforgeability. The consensus algorithm is called Quantum Secure Yet Another Consensus (QSYAC), which is a variant of Hyperledger Iroha's YAC. YAC is a vote-based consensus. QSYAC utilizes the quantum channel between every two peers for key exchange and classical channels for data transfer. The signature is based on keys delivered via QKD, i.e., even a quantum adversary cannot forge it.

Iovane[93]: Computational quantum key distribution (CQKD) on decentralized ledger and blockchain. This is essentially a distributed and decentralized QKD protocol on a blockchain. They have emphasized on how BB84 [78] realizes absolute security in distributing the key for Vernamm's cipher (One Time Pad) and symmetric cryptography in general. The network assumes quantum

and classical channels. The first section distributes the quantum key distribution process among a subset of network nodes, i.e., Alice (sender) and Bob (recipient), rather than concentrating the process around their nodes, delegates, and distributes the key distribution work among available network nodes. The roles those nodes can play are Quantum Spin Generator (QSG), Base Generator (BG), Quantum Photon Polarizer (QPP), Photon Fusion Engine (PFE), Quantum Photon Meter (QPM), and Quantum Photon Collider (QPC). QSG generates up and down spins randomly, whereas BG generates random bases: diagonal or rectilinear. In those bases, for those spins, QPP polarizes photons. PFE fuses these polarizations together. QPM measures Alice's polarizations at the basis generated for BoB by BG. QPC compares two strings of polarization and lets Bob and Alice know the matching and mismatching indices. Nodes are allocated dynamically. An adversary (Eve) cannot synchronize with all nodes without having complete control of the network, which is impractical. Even if she sniffes components of the key from PFE, QPM, QPC, she cannot know who to report them to: Bob or Alice. Eve can pierce nodes, construct addresses given by Bob and Alice could and theoretically construct the key, although practically impossible. This is due to the centralization of the network, although distribution is achieved. Therefore, in the second section, decentralization of distributed ledgers is utilized. This blockchain is explained in their later work.[94] They claim further decentralization can be achieved by incorporating two computational quantum components, named Quantum Photon Transmission Component (QPTC) and Quantum Photon Receiver Component (QPRC).

Iovane[94]: MuReQua Chain: Multiscale Relativistic Quantum Blockchain. The democracy and the randomness of a block creator and the assignment of a new block are solved by using a multiscale approach of Complexity Theory and Quantum and Relativistic Mechanics. The consensus (block validation and assignment) is based on an extended probability environment. Authentication is based on the QKD protocol named CQKD, based on computational photons (quantum packets of information exchanged by two operators) from the work by Iovane[93]. An optimized version of that CQKD is described in this work, which is included under that work itself. The negotiation within the consensus protocol includes a bidding and a price model where a price has four characteristics: Probability, Plausibility, Credibility, and Possibility. Then follows a simple statistical negotiation model with a buyer, a seller, and market makers as shown in Figure 11.

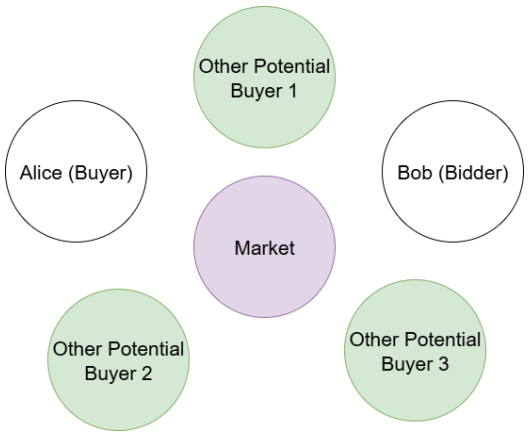

Figure 11: Negotiation parties [94]

This negotiation model has been customized for blockchain as a consensus mechanism, which then rewards miners with a new cryptocurrency. They claim this blockchain is multiscale (scalable), quantum (quantum-resistant), and relativistic (fully distributed and decentralized). It needs to be noted that this paper completes the blockchain proposed by Iovane[93]. The seller in the negotiation model is the miner who mined the previous block and is waiting for the reward in the consensus. Buyer is the candidate for the new block assignment to be mined. Market makers (other bidders) are competitors to the buyer. In transforming the negotiation model to a consensus protocol, certain constraints have been introduced. A consensus mechanism is unfolded henceforth. Nonetheless, certain aspects may still require clarification.

4.2.2. Hybrid Quantum Blockchain (Signature-based)
Wang et al.[82]: Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm. Proposed by Wang et al.[82] is a blockchain algorithm based on asymmetric quantum encryption and a stake vote consensus algorithm. The consensus algorithm is based on the Delegated Proof of Stake (DPoS) with Node Behavior and Borda Count (DPoSB). The quantum digital signature technology is based on the QSCDff problem. DPoSB is used to generate blocks by voting, while the quantum signature applies quantum one-way functions to guarantee the security of transactions. DPoS, unlike other proof-based consensus mechanisms, does not rely on computational capabilities. Therefore, there's no mining competition.

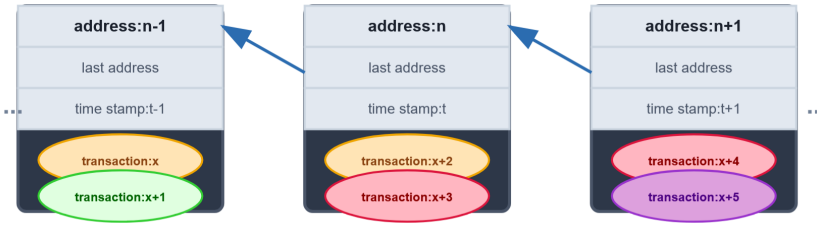

Figure 12: Blockchain structure [82]

Instead of hash pointers, blocks point to the address of the previous block as shown in Figure 12. The sending node signs a transaction with his private key, which is verified by other nodes utilizing his public key. The consensus protocol has a phase where the nodes elect a set of witness nodes that participate in the consensus and block creation. Voting calculates a Borda score for candidates. Ones with the highest scores become witnesses. Nodes sign transactions through a quantum one-way function based on the QSCDff problem. Wang et al.[82] present the quantum signature protocol (see Paragraph 4.1.2). Transactions (classical bit strings) verified by $\frac{2}{3}$ of witnesses can be packaged into a blockchain by the present witness, i.e., the block-producing witness for the current duration in the cycle. This framework is secure from intentional disturbing of block production by malicious nodes due to the voting in DPoS — a low Borda score results in losing the election. Since the chain is not formed by hash pointers and there's no mining race, computational power attacks such as Grover's attack to rewrite the chain are not effective. According to the hardness of the QSCDff problem proved by Wang and Yu[82], the problem of distinguishing quantum states without π cannot be solved in polynomial time. Thus, it can be claimed that the blockchain has quantum information-theoretical security. A security comparison against an entanglement-based signature is given by the authors.

Bennet and Daryanoosh[95]: Energy-efficient Mining on a Quantum-Enabled Blockchain Using Light. The mining and consensus of this framework depend on the relationship between entanglement and trust. All quantum information transmitted is encoded into photonic qubits over fiber-optic infrastructure.

> These research outcomes have demonstrated that entanglement can be used as an indicator of device trustworthiness, such that,

> under appropriate circumstances, if entanglement is observed, then a device's behavior may be certified as trustworthy. [95]

The authentication round utilizes a decoy-state variant of the Quantum Secure Authentication (QSA) protocol. QSA is a quantum cryptographic security primitive for the purposes of identification, authentication, read-proof key storage, key distribution, tamper detection, anti-counterfeiting, etc. The network consists of clients and quantum servers. Servers have photonic entanglement generation sources, where clients have quantum modems for authentication of themselves and quantum state measurements. The embedded photonic key on these modems can be used to derive addresses for clients, and due to the no-cloning theorem, they cannot be spoofed. In the mining round, clients need to elect a subset of servers as a consortium to participate in block creation and consensus. Every server proposes a candidate block, and clients choose a server they want to work with and generate entanglement based on reputation. Hence, a server has a team of clients for the block creation round. Servers with the most entanglement generated are selected as the consortium to participate in the consensus. A modified delegate Byzantine Fault Tolerance (BFT) protocol is utilized. Due to the election is based on entanglement, consensus is also known as Proof of Entanglement (PoE). This PoE and verification of it for a server consists of parameters from the measurement data from the client team of the entangled photons sent to them by the server. These parameters include heralding efficiency η of the quantum server and the EPR steering parameter S_n. The delegated BFT elects a "speaker" who has the opportunity to create the block from his team. If his PoE is detected to be falsified, a new speaker is elected, and the offender's reputation diminishes. The rest of the work has a case-specific security analysis.

4.2.3. Fully Quantum Blockchain

What defines a quantum blockchain is the chain itself being formulated by quantum states; the blockchain needs to be stored in quantum registers. In much of the literature, a one or two-particle quantum system constitutes a block. Most popular and earlier quantum blockchain conceptualization is to encode the blockchain into a temporal Greenberger–Horne–Zeilinger (GHZ) state of photons that do not coexist simultaneously.[96] The entanglement between blocks is temporal, not spatial. The newer popular approach is to build the blockchain as a weighted quantum hypergraph state [97]. Banik et

al. [98] have presented a concept of a blockchain on GHZ states. Quantum Random Number Generation (QRNG) and ϑ - protocol are used here to achieve consensus, where QRNG ensures the randomness in selecting a block producer. After this election, a distributed consensus is reached, and blocks containing validated transactions are created. They have implemented and tested this concept on the IBM Q quantum computer. An overview of this scheme is depicted in Figure 13.

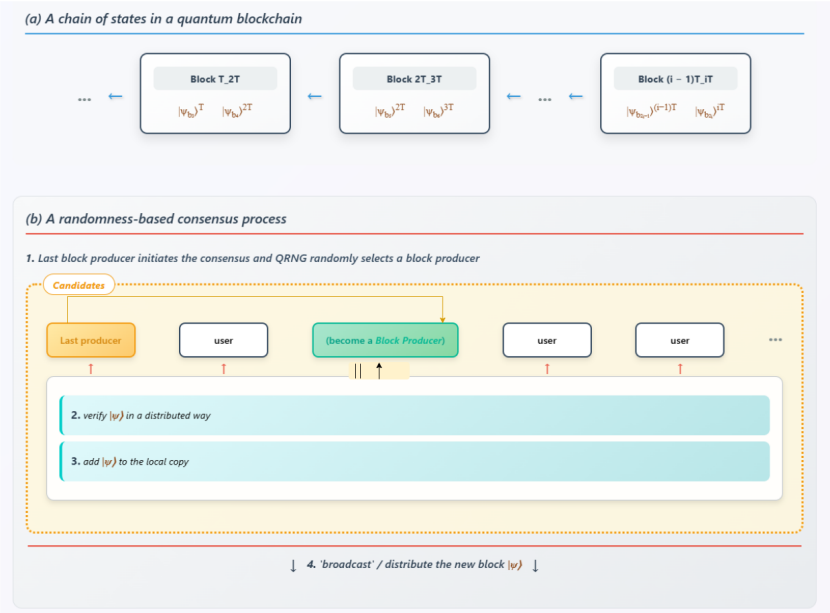

Figure 13: Fully quantum blockchain overview

Rajan and Visser[96]: GHZ state time temporal entanglement blockchain. Given two classical bits xy, the protocol next prepares the corresponding spatially entangled Bell state:

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

The decoding process can extract the classical bit string, xy, from $|\beta_{xy}\rangle$. The encoding process converts a bit string r_1r_2 into a temporal Bell state, generated at a particular time, $(t = 0)$, is given by:

$$|\beta_{r_1r_2}\rangle_{0,\tau} = \frac{1}{\sqrt{2}}\left(|00\rangle|r_2\rangle_\tau + (-1)^{r_1}|10\rangle|\bar{r}_2\rangle_\tau\right).$$

The superscripts mark the time at which the photon is absorbed. Three chronological blocks would be:

$$|\beta_{00}\rangle^{0,\tau}, \quad |\beta_{10}\rangle^{\tau,2\tau}, \quad |\beta_{11}\rangle^{2\tau,3\tau}.$$

They can be fused using entanglement in time [99] to form a chain by projecting new blocks continuously to a growing GHZ state. The state of the quantum blockchain at $t = n\tau$ (from $t = 0$) is given by:

$$|\mathrm{GHZ}_{r_1 r_2 \ldots r_{2n}}\rangle_{0,\tau,\tau,2\tau,2\tau,\ldots,(n-1)\tau,(n-1)\tau,n\tau} = \frac{1}{\sqrt{2}} \left(|00 r_1^\tau r_2^\tau \ldots r_{2n}^\tau\rangle + (-1)^{r_1} |10 \bar{r}_2^\tau \bar{r}_3^\tau \ldots \bar{r}_{2n}^\tau\rangle\right).$$

Subscripts on the left side denote the concatenated string of the entire blockchain, while superscripts denote the timestamps. The scalability, even in a scenario of quantum internet and widespread quantum infrastructure, is questionable, given that only 2 bits are encoded into a block. They have assumed a quantum network for communication with a QKD-based signature/encryption scheme from another work. To prevent dishonest blocks from adding blocks, ϑ - protocol has been utilized to achieve consensus: a random node in the quantum network can verify that the untrusted source created a valid block (spatial GHZ state). All the nodes in the network share their measurements of the new block shared by the untrusted node with the random verifier, where that node determines the admissibility of the n-qubit block. The quantum advantage is that the full local copy of the blockchain is destroyed if one tampers with a single block (entanglement). This is in the spatial entanglement case. But the temporal entanglement chain is more secure in the sense that an attacker cannot access older blocks, for they no longer exist. The authors claim this framework does not provide Byzantine fault tolerance.

Banerjee et al.[97]: Quantum Blockchain on Weighted Hypergraph States. Quantum hypergraph states are a group of highly entangled, multipartite quantum states that are constructed on a mathematical hypergraph.[100] Quantum particles sit as vertices where edges represent multipartite entanglement.

For each hyperedge, a controlled-Z operation has been performed on the connecting qubits. The state in Figure 14 can be written as:

$$|\psi\rangle = C^2_{(1,2,3,4,5)} Z C^2_{2(1,2,3)} Z |+\rangle^{\otimes 5}.$$

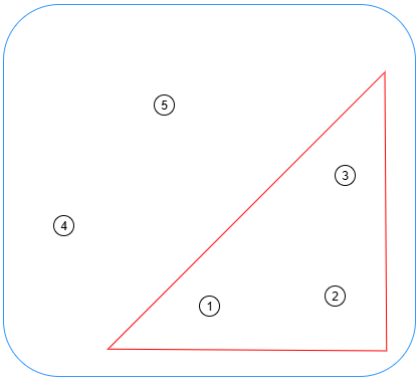

Figure 14: Hypergraph state: 5-hypergraph, 3-hyperedge, 5-hyperedge. [97]

Local unitary operations carried through classical communication (LOCC) do not alter the entanglement of the state under consideration. The authors have referenced the work that proved that using local applications of Pauli operations on the k^{th} qubit, one can remove all the (N-1) edges such that an n-qubit hypergraph contains only an n edge. A weighted hypergraph state can be represented by a hypergraph where each hyperedge carries a weight:

$$|\psi\rangle = \sqrt{\frac{1}{2^N}} \sum_{x \in (0,1)^N} e^{i\pi f(x)} |x\rangle,$$

where $|x\rangle$ represents the computational basis state. In the blockchain, they have used the phases of the new qubit, i.e., block, carried by the hyperedges of the weighted hypergraph states (i.e., weights) to encode the classical information in the hypergraph state. Nodes only use local operations and classical communications over a quantum secure channel using a QKD protocol to build the chain according to an agreed-upon consensus. One qubit constitutes one block. A classical block is a bit string. This string is equivalent to decimal p. This p is converted into a phase factor ϑ_p by a bijective function. Consensus involves all nodes verifying whether ϑ_p satisfies predefined criteria which are crucial in measuring and reconstructing the chain, i.e., when measured, the chain collapses, where with the knowledge of the genesis block's phase and subsequent phases adhering to the criteria, it is possible to reconstruct the blockchain. The peer who creates the genesis block has $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Then he applies the rotation $S(p)$ with ϑ_{p_1} to create the first block:

$$|\psi_1\rangle = S(p)\,|\psi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0\\ 0 & e^{i\theta_p}\end{bmatrix}|\psi\rangle == \frac{1}{\sqrt{2}}\,|0\rangle + \frac{e^{i\theta_{p1}}}{\sqrt{2}}\,|1\rangle\,.$$

The 3-qubit entangled chain is as follows:

$$C^2_{12,3}Z(|\psi_{12}\rangle \otimes |\psi_3\rangle) = \frac{1}{2}\Big(|000\rangle + e^{i\theta_{p3}}\,|001\rangle + e^{i\theta_{p2}}\,|010\rangle + e^{i(\theta_{p2}+\theta_{p3})}\,|011\rangle$$
$$+ e^{i\theta_{p1}}\,|100\rangle + e^{i(\theta_{p1}+\theta_{p3})}\,|101\rangle - e^{i(\theta_{p1}+\theta_{p2})}\,|110\rangle + e^{i(\theta_{p1}+\theta_{p2}+\theta_{p3})}\,|111\rangle\Big). \quad (5)$$

If a proposed block does not pass the above verification, the node would be considered untrustworthy. Due to entanglement, an attacker measuring a block would result in the collapse of the entire chain. If they attempt to mutate a block, i.e., change the phase, the phases of the chain would no longer be valid under the defined consensus criteria and would result in the owner of that local copy reconstructing the original blockchain.

Ikeda[101]: qBitcoin — A Peer-to-peer Quantum Cash System. This is a decentralized online quantum cash system. Quantum teleportation technology is used for coin transactions, which prevents the owner from keeping the coin data after sending it. In qBitcoin, double-spending never happens due to no-cloning. qBitcoin is based on a quantum chain, instead of blocks. A digital signature is part of the protocol; it is a P2P network still. A coin is a pair of classical and quantum states $c_i = (r_i, |\psi_i\rangle)$ where i is a serial number and r_i is a transaction record made of classical bits. The transaction is done by passing c_i. The coin and a bank statement are transmitted via teleportation[87], which is a method to send quantum information via classical networks. To do secure related classical communication, the two parties use a QKD implementation.

Transactions are approved once if signature of the sender is verified. The quantum signature protocol of Gottesman and Chuang[85] described in Paragraph 4.1.2 is used for transaction authentication. It is based on a one-way function that satisfies:

$$k \mapsto |f_k\rangle \quad \text{(easy)}$$
$$|f_k\rangle \mapsto k \quad \text{(impossible)}.$$

Public key $|f_k\rangle$ needs to be copied and distributed to network nodes to verify signatures, but the number of copies should be limited since with too

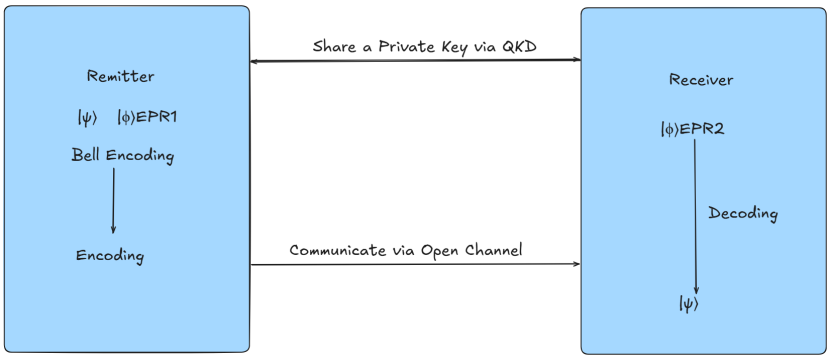

Figure 15: qBitcoin remittance [101]

many copies, the risk of private key k being discovered increases according to Holevo's theorem. A sender and a receiver share a private key using QKD as shown in Figure 15. The sender's remittance request contains the record r, signature $s = (k, |f_k\rangle)$, and encoded $|\psi\rangle$ of the coin. A random set of verifiers receives the public key $|f_k\rangle$; if the signature is approved, a verifier updates the public record. To steal a coin, an adversary would have to obtain the private key of the sender of coins. This is impossible due to QKD being absolutely secure against eavesdropping. Private keys — which are not secret (QKD) — are generated per transaction and therefore bear no correlation to the sender. Blind quantum computation is proposed for users without quantum computers.

Li et al.[32]: Efficient Quantum Blockchain with a Consensus Mechanism QDPoS. This framework's consensus protocol is Quantum Delegated Proof of Stake (QDPoS). It is based on quantum voting. Unlike PoW or PoS, this is not defined on computational capabilities, and therefore, the 51% is not a concern. The blockchain itself is a weighted hypergraph state[97] (see section 4.2.3). There are two entanglement states in a quantum voting protocol that are useful in consensus. Wang et al.[102] describe this voting protocol.

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

where

$$|j'\rangle_{\mathcal{F}} = \mathcal{F}|j\rangle_C = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} e^{\frac{2\pi ijk}{m}} |k\rangle_C$$

and $\{|j\rangle_F \mid j = 0, 1, \ldots, m-1\}$ is the fourier basis.
The other state is;

$$|\eta_n\rangle \equiv \frac{1}{\sqrt{n!}} \sum_{S \in P_n^n} (-1)^{\tau(S)} |s_0\rangle |s_1\rangle \cdots |s_{n-1}\rangle, \tag{6}$$

where P_n^n is all permutations of $\{0, 1, \ldots, n-1\}$, $S = s_0 s_1 \cdots s_{n-1} \in P_n^n$, and $\tau(S)$ is the inverse order of S. Quantum voting is immune to quantum attacks because it provides information-theoretic security rather than computational complexity security. Similar to DPoS, QDPoS voting process elects a group of representatives for block creation. The original voting protocol [102] has been modified by the authors to accommodate positive, negative voting, and abstaining from voting. The distribution of quantum states is done by the distribution center CA. Ballots are generated by measuring the distributed qubits. The collective ballot in the quantum voting is a matrix similar to almost all e-voting protocols, where a row corresponds to a voter's ballot. Elected nodes generate blocks cyclically (shown in Figure 16) for chronological fixed durations of t.

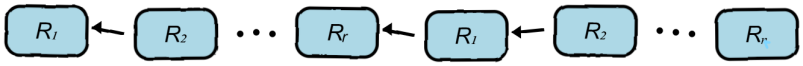

Figure 16: Cycle of block generation [32]

After a cycle, an election could be performed again. The signature scheme is the quantum signature presented by Gottesman and Chuang [85] (see section 4.1.2). Transactions are signed and released to the network, where any node with corresponding public keys can verify. The node N_i generates the signature $S_i(T_i)$ of the transaction T_i using the quantum private key sk_i and broadcasts $(T_i, S_i(T_i))$ to the network. Then voting takes place. The bijective function to create the blockchain is agreed upon by all the nodes. The representative node selected in the current t of the cycle collects transactions

occurring in t, verifies them, and creates the one qubit quantum block for using the bijective function and rotation gate:

$$|\psi\rangle = R(\theta_M)|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta_M}|1\rangle\right),$$

where M contains the transaction messages that have been verified. θ_M is determined by the bijective function, such that $F(M) \leftrightarrow \theta_M$, and $R(\theta_M)$ represents a rotation operation by the angle θ_M. Then θ_M is passed to other representatives, where if more than half of them agree that the consistency of the chain is preserved, θ_M is broadcasted to the whole network so that all local chains can be updated. The authors claim the QDPoS consensus is more inclined to consortium chains. Blockchain tempering security is described by Banerjee et al.[97] (see section 4.2.3), while signature forgery is addressed by Gottesman and Chuang [85] (see section 4.1.2). Trapped qubits are inserted into the distributed quantum states of the voting process to prevent attackers from manipulating ballots.

Mayers[103]: Quantum Bitcoin. This is an attempt to transform Bitcoin to run on a quantum computer, and it has immediate local verification of transactions. Therefore, computationally intensive methods of recording every transaction on the chain are unnecessary. Blocks do not contain standard transactions, only classical descriptors of the newly minted quantum bitcoin. They have used a quantum state as the coin and endowed it with classical information to facilitate verification. They first described a blockchain-less mini scheme based on a hidden subspace to mint and verify a single quantum bitcoin. They define A as a $n/2$-dimensional sub-space of F_n^2. The quantum Bitcoin states look like:

$$|A\rangle = \frac{1}{\sqrt{|A|}} \sum_{x \in A} |x\rangle.$$

The minting function utilizes a subspace generator while the verifier function accepts a bitcoin in the format s, p where s is a serial number and verifies the serial number for the quantum state p. Then comes the standard quantum Bitcoin scheme for unlimited minting and a blockchain. This scheme has a digital signature scheme. This time, the coin c is in the form (s, ρ, σ), where the s is a classical serial number, ρ a quantum state, and σ a classical digital signature. The signature can be verified using the public key associated with the serial number, from where the mini scheme's verification can

be used to verify the coin. One key advantage of Quantum Bitcoin is instant transaction finalization, unlike classical Bitcoin transactions, which require blockchain recording. The no-cloning theorem inherently prevents counterfeiting by ensuring that quantum states cannot be duplicated. Miners are untrusted but trusted as a whole. The minting process generates a new key pair, generates a quantum bitcoin, and signs the serial number. Then it appends the serial number to the ledger along with the public key. A miner could use the same private key to sign multiple coins (double minting). In Quantum Bitcoin, there is no record of ownership and transaction records like classical Bitcoin, so doubly-mined quantum Bitcoin would go unnoticed since only the minting is recorded. A mining protocol with two stages, with intermediary coins known as "shards" is proposed to counter double minting. This construction assumes that a majority of miners are honest, i.e., discard private keys after mining. Verification is modified accordingly. The coin c' is of the form $(s_1, \rho_1, \sigma_1, \ldots, s_m, \rho_m, \sigma_m, \sigma_0)$, where s_i are classical serial numbers, ρ_i are quantum states, and σ_i (including σ_0) are digital signatures. Verification is analogous to the previous case. Then, they have proved the counterfeiting and double minting resistance of their application.

4.2.4. Quantum Blockchain Applications

Alharby et al.[86]: A Blockchain Smart Contract Based on Light-Weighted Quantum Blind Signature. The signature scheme is described under quantum signatures (see section 4.1.2). Apart from the signature being quantum, smart contracts depend on quantum information being transmitted. Figure 17 shows the smart contract architecture, which consists of five layers.

This scheme can meet various contract conditions, including payment rights, mortgage, QKD, privacy, and confidentiality, and on the other hand, it can lower transaction costs, execution costs, arbitration costs, transaction losses from quantum attacks, and contract fraud, according to the authors. This architecture has predefined rules: digitization of all products and services, mediums of exchange, and multiple distributed databases (distributed ledger). Quantum information transmission in this work is mainly used to establish and transmit quantum keys in smart contracts, instead of transmitting plaintext or ciphertext.

Figure 18 shows the smart contract lifecycle. Contract development involves negotiating quantum keys, rules, and coding. Verified contracts are tested and distributed across the blockchain. Execution includes triggering, quantum blind signature verification, and block creation. Valid contracts pro-

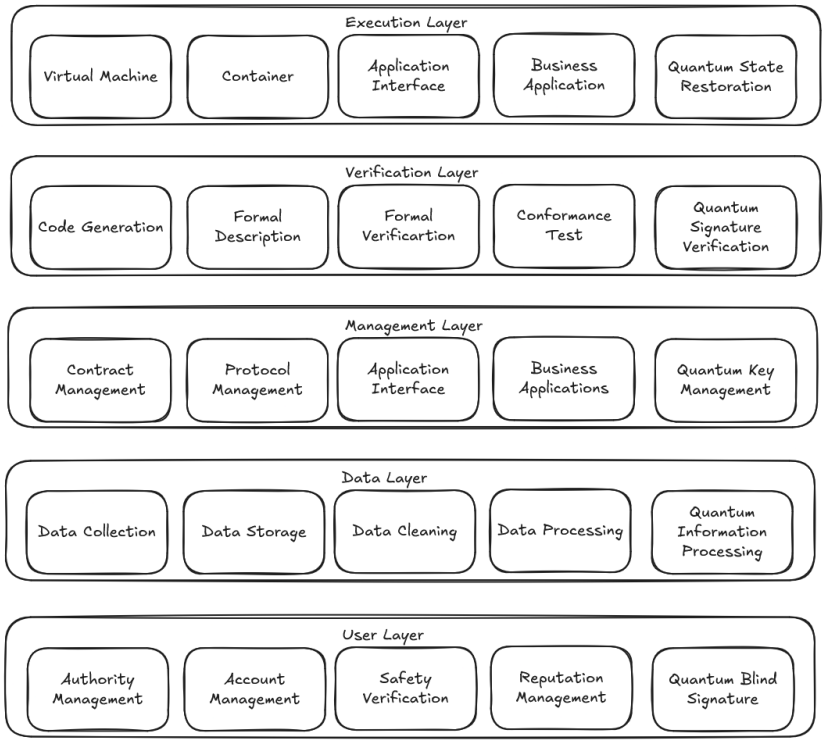

Figure 17: Smart contract architecture [86]

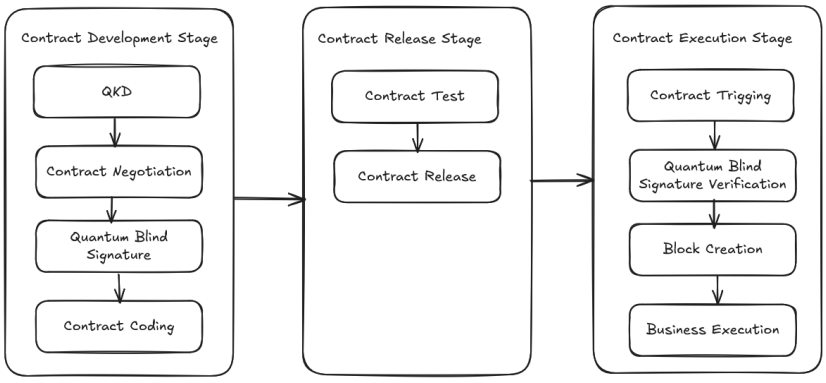

Figure 18: Smart contract life cycle [86]

ceed to consensus and execute automatically; invalid ones fail. Each trader's transaction follows pre-programmed smart contracts. The block creator first blinds the transaction message, which is then signed and released by the

trader. The signature is later revealed, verifying the trader's original text. Quantum blind signatures ensure privacy while allowing the block creator to confirm authenticity. The quantum blind signature of a smart contract is decentralized, can be self-sufficient, blind (signers cannot know the content of the message text while performing the signature on a transaction), unforgeable, and non-repudiable. The creator of the block would decrypt the signature to obtain the signed transaction (smart contract) after receiving it from the trader. A measurement comparison of signature qubits would reveal the executability of the smart contract. Once the entangled pairs are shared, contract negotiation begins. After the verification of the signature, the block will be created and broadcasted over the network, where the smart contract would execute naturally.

Sun et al.[104]: A Simple Voting Protocol on Quantum Blockchain. The authors claim this protocol exhibits the vital properties of voting protocols: anonymous, binding, non-reusable, verifiable, eligible, fair, and self-tallying. Their goal was to propose such a quantum blockchain-based application that is implementable with today's technology. The quantum blockchain is adopted from Sun et al.[89] (see section 4.2.1) and Kiktenko et al.[5] (see section 4.2.1). The voting process requires QBC. Each pair of nodes is connected by a secure quantum channel, whereby they perform QKD and a classical unsecured channel. Classical data of an update to the chain is sent via classical channels to all miners, while the quantum data of the update takes quantum channels. Each miner checks the consistency of the update with their copy of the chain. Then, a Byzantine agreement is used to achieve consensus on the admissibility of the update. They have referenced their own CSQBC protocol [91] for bit commitment in here.

Voters performing the ballot constitutes the commitment phase, where the tallying takes place in the announcement. As in most e-voting protocols, the collective ballot of all voters is in the form of a matrix where the i^{th} row is the ballot of voter i. Voters use quantum secure communication (QSC) to distribute the matrix. Voters commit their masked ballots to miners as shown in Figure 19. In the announcement phase, voters reveal their ballots to miners so that miners can perform Quantum Honest Byzantine Agreement [89] to come to consensus regarding the tally. Anonymity of the vote is established because QSC prohibits other voters from knowing the entire matrix: they only see masked ballots of others. Due to QKD authentication, one cannot change another's vote, and cannot change their own due to the binding

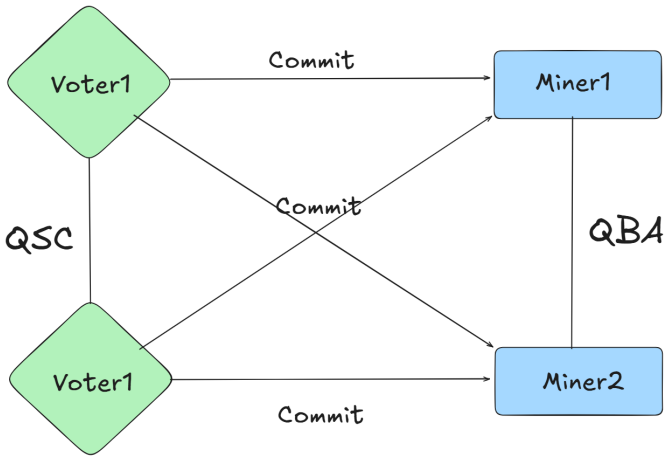

Figure 19: Voting on Quantum Blockchain [104]

property of QBC. Voters cannot append two ballots since double spending is impossible on a quantum blockchain. A voter can verify that their ballot is on the chain since the blockchain is transparent. Only authenticated voters can successfully communicate with the miners.

Sun et al.[105]: Lottery and Auction on Quantum Blockchain.

> Our protocol of lottery satisfies randomness, unpredictability, unforgeability, verifiability, decentralization, and unconditional security. Our protocol of auctions satisfies bid privacy, posterior privacy, bids' binding, decentralization, and unconditional security.[105]

In Sun et al.[92], the lottery protocol is limited to two parties, whereas a multiparty scheme is proposed in subsequent work by Sun et al.[105]. Unconditional security in these protocols is the notion of an adversary with unlimited computing capabilities being unable to attack successfully, i.e., in polynomial time. They claim that no auction protocol has provided both decentralization and unconditional security before their protocol. The quantum blockchain here is adopted from Sun et al.[92, 104] (see section 4.2.1 and section 4.2.4) and Kiktenko et al.[5] (see section 4.2.1). They assume each pair of nodes has a quantum channel and a classical channel. They can establish secret keys by using QKD. Nodes initiate new transactions or messages to append data to the blockchain. Miners verify consistency with

their local ledger, assess its validity, and reach a consensus on the correct update through a consensus algorithm. In this paper, they have used a QBC protocol from their previous paper. In the lottery, players purchase tickets by committing a bit string to all miners in QBC as shown in Figure 20. Miners run a consensus on ticket validity after they are revealed. A winning ticket is formulated, and players are rewarded by the distance to the winning ticket.

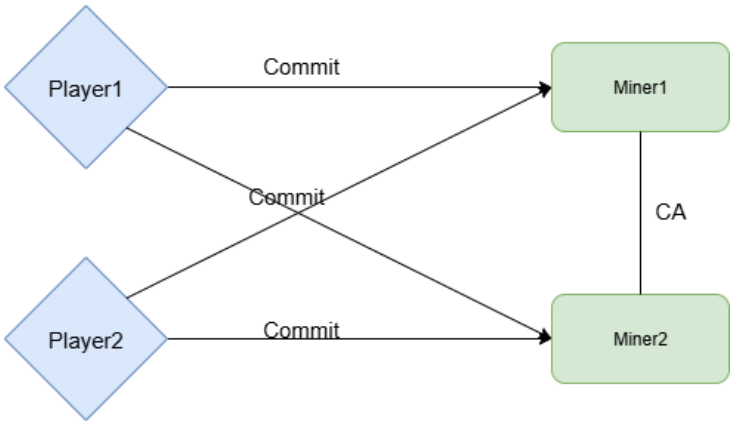

Figure 20: Lottery protocol on QBC[105]

In the auction, there's a seller, a set of buyers, and a set of miners. All buyers commit their bid to the seller and all miners. Then, buyers reveal the bids to the seller, where the seller determines the winning bid and the winner. Then, to convince the miners that the seller has chosen the actual winner and winning bid, the seller and miners participate in a consensus algorithm similar to QHBA [89] that accounts for dishonest seller or miners. The consensus is then added to the blockchain. The rest of the work analyses how their lottery and auction meet their respective required properties.

Yan et al.[14]: Decentralization using quantum blockchain — A theoretical analysis. The blockchain itself is identical to Rajan and Visser[96] (see section 4.2.3). QRNG chooses a random verifier to verify transactions and create a block. θ-protocol is then employed to achieve consensus among other nodes regarding the validity of the block. What they have proposed here is an identity framework on the quantum blockchain (QBIF). The purpose is to manage identities without forgery and to preserve privacy. Users control their identities. An identity has a unique ID and attestations, which are proofs of user statements about attributes such as birthdays and income. A

verifying party can verify based on the signature of an issuer without actually discovering the value of the attribute. A bank can verify a threshold for an income without looking at the actual income; these attributes are private to users. Figure 21 shows the three roles in QBIF: identity owners, identity issuers, and identity verifiers. A bank may issue an attestation about a user's financial attributes. The verifier does verifications to provide the owner with services. Ownership is marked by double signatures. Attestations on this blockchain are quantum states — Quantum Identity Attestation (QIA). If ψ is an n-bit string of attestation, a QIA can be:

$$L\phi|0\rangle^{\otimes n} = |\psi\rangle = |b_1 b_2 \dots b_n\rangle.$$

This is double-signed by the owner and issuer. It is assumed there are quantum channels between every node. Issuers and verifiers are block producers.

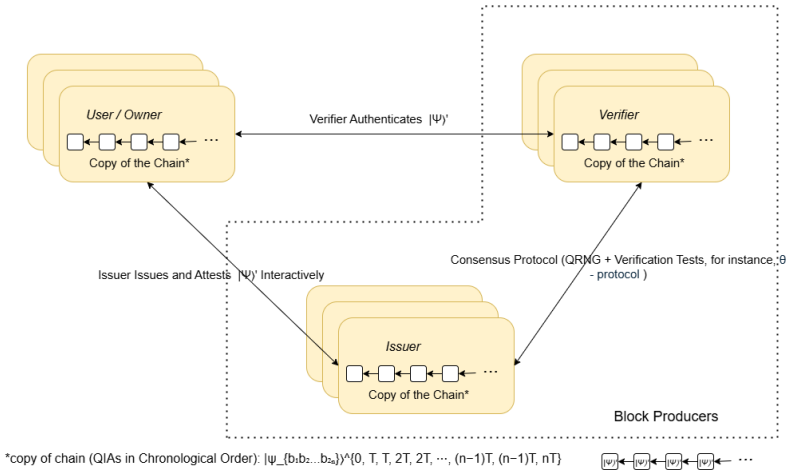

Figure 21: Identity Blockchain roles [14]

Once a QIA is put on the chain, the owner can initiate an action with a verifier by sending the location of the signed QIA on the blockchain. Off-chain communication and storage for IA will be done on classical systems. The distributed verification for the new block by the elected producer keeps the chain validated even in the presence of dishonest nodes. This double signed QIA $|\psi\rangle'$ is verified by all nodes, but even a valid QIA can fail verification due to entanglement fidelity. The output of the majority of the network is accepted. This framework uses the public key signature scheme above under Yang et

al.[83] and Liang and Yang[84] (see section 4.1.2). Therefore, security lies on the quantum trapdoor function. The chain is tamper-secure as mentioned in Rajan and Visser [96]. QIAs do not have actual identity information. Therefore, the leakage of off-chain IAs is not a significant compromise.

Gupta et al.[106]: End to End Secure e-Voting Using Blockchain and Quantum Key Distribution. This voting protocol, as claimed by the authors, possesses all properties of an acceptable e-voting mechanism: Receipt-Freeness, Justice, Data Reliability, Privacy/Voter Anonimity, Reliability/Robustness, Individuality, and Verifiability. The application is based on a classical blockchain with quantum cryptography for quantum security — only the block date signatures/symmetric key encryption. A block contains the Voter's ID, Vote (a poll for preference), Hash of the previous block, Voter Signature, and Timestamp. Apparently, this blockchain is a permissioned (a less strict form of private) blockchain where central authorities perform authentication of users. However, the blockchain consensus, including block data authentication, is not clearly provided. The paper presents the flow diagram for voting, from registration/signing in to storing the vote on the chain to displaying results. They have proposed using QBC-based authentication or quantum digital signatures instead of QKD. The rest of the paper explores the current state-of-the-art in blockchain-based e-voting.

5. Critical Analysis of the Work

This section critically evaluates the findings of the reviewed studies, highlighting limitations, biases, and opportunities for improvement. It includes our personal assessments and critiques.

5.1. Post-Quantum Blockchain

We have explored post-quantum research regarding a few segments of the blockchain framework: signature, consensus, wallets, and hashing. Figure 22 illustrates the composition of post-quantum blockchain literature in terms of their cryptography families.

5.1.1. Strengths of Existing Research

There are public key cryptosystems that have been standardized by NIST as of August 2024: Dilithium, Kyber, and SPHICS+. Therefore, arguably, they are the most secure among their competitors. Therefore, it can be concluded that, according to NIST, post-quantum blockchains based on these

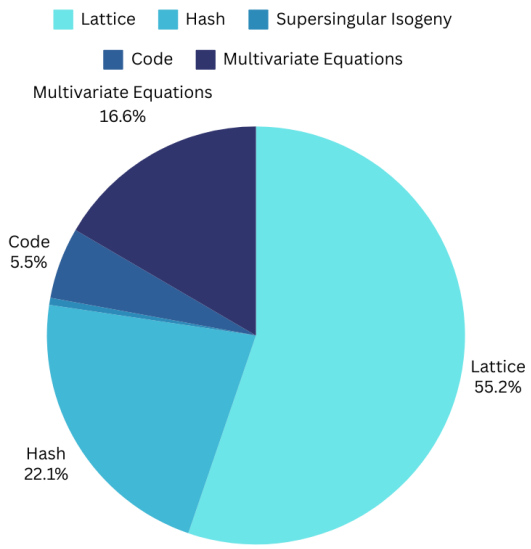

Figure 22: Distribution of Post-Quantum Blockchain literature

schemes offer the highest resistance to both quantum and classical attacks. Although not focused on integrating into blockchains, there are unconditionally secure hashing algorithms based on quantum technologies against quantum attacks.[36, 37]

5.1.2. Weaknesses and Gaps in Literature

What is obvious as a weakness in the literature is the lack of extensive work on integrating quantum hashing into post-quantum blockchain. There are post-quantum blockchains proposed in the literature using classical hash functions with larger hashes than classical blockchains. [50, 56, 72] Also, the biggest weakness in post-quantum blockchain in general is that they are still protected by classical cryptosystems that are based on computational difficulty and unproven to be insecure — they do not harness the absolute security of quantum mechanics.

5.1.3. Challenges and Limitations

In integrating post-quantum cryptography into blockchain, the biggest challenge is to choose different families of cryptography, balancing advantages and disadvantages. For instance, lattice-based and hash-based primitives offer efficiency and performance with less algorithmic complexity, smaller key

sizes, and ciphertexts, but offer less security at the same security levels compared to code-based counterparts, which are heavier in terms of complexity and sizes. Table 3 summarizes key size, speed, and adoption status for each scheme.

Table 3: Comparison of Post-Quantum Cryptosystems

Scheme	**Key Size**	**Speed**	**Status**
Lattice	Small (1-2 KB)	Fast	Practical (NIST)
Code-Based	Huge (100KB+)	Slow	Limited Use
Multivariate	Medium (20 KB)	Moderate	Some Broken
Isogeny	Tiny (200 B)	Very Slow	Mostly Broken
Hash-Based	Small	Fast (Signing)	Viable (SPHINCS+)

Another challenge is the lack of awareness and physical resources in the case of quantum blockchain. There are cryptologists and blockchain researchers who are yet to venture into post-quantum cryptography and blockchain. Also, the lack of hardware and access to cloud hardware deters empirical validation since simulators cannot provide the same functionality and credibility.

5.2. Quantum Blockchain

For this, we have taken a different approach from the exploration into post-quantum blockchain. We have explored some quantum cryptographic primitives useful for quantum blockchain and performed an analysis of many works up to date. Figure 23 illustrates the distribution of quantum blockchain literature in terms of its technical composition.

Table 4: Quantum Blockchain Technicality

Category	**Reference**	**Title**	**Technology**

Category	Reference	Title	Technology
Hybrid Quantum Blockchains (QKD)	[5]	Quantum Secured Blockchain	QKD transaction authentication, Symmetric key encryption, Transaction aggregation into classical blocks, Broadcast protocol, Larger hash than classical blockchain, Classical BFT, Fibre QKD
	[89]	Quantum-enhanced Logic-based Blockchain I: Quantum Honest-success Byzantine Agreement and Qulogicoin	Quantum protection and quantum certificates in transactions, QHBA consensus, QKD, Toeplitz keyed hashing, classical transaction certificates, Classical transaction hash validation, QSDC, Quantum Shamir's 3-pass
	[92]	Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic	Vote-based consensus, QKD signature, Scripting language for smart contracts, Quantum resistant lottery protocol, USS, Toeplitz hash MAC, TGS, QSYAC
	[93]	Computational Quantum Key Distribution (CQKD) on Decentralized Ledger and Blockchain	Quantum/classical channels, Distributed, decentralized QKD, QSG, BG, QPP, PFE, QPM, QPC, QPTC, QPRC

Category	Reference	Title	Technology
	[94]	MuReQua Chain: Multi-scale Relativistic Quantum Blockchain	All from section 4.2.1, CQKD, Computational photon, Negotiation-based consensus, Cryptocurrency reward
Hybrid Quantum Blockchains (Quantum Signature)	[82]	Quantum Blockchain Based on Asymmetric Quantum Encryption and a Stake Vote Consensus Algorithm	QSCDff Quantum Signature, DPoS with node behavior, Borda Count, Quantum one way function, Entanglement-based signature
	[95]	Energy-Efficient Mining on a Quantum-Enabled Blockchain Using Light	Photonic entanglement, Photonic qubit transmission over fibre, Decoy state QSA, Entanglement generators, Quantum modems, Embedded photonic key, PoE, Delegated BFT, EPR steering parameter, Heralding efficiency
Fully Quantum Blockchain	[96]	GHZ State Time Temporal Entanglement Blockchain	Temporal Bell entanglement, Entanglement in time, GHZ state, QKD signature, QRNG for block validation, ϑ - protocol consensus
	[97]	Quantum Blockchain on Weighted Hypergraph States	Quantum weighted hypergraph, Multipartite entanglement, LOCC Unitary operations, Encoding into phases, Decimal to phases bijective, QKD classical communication

Category	Reference	Title	Technology
	[101]	qBitcoin - A Peer-to-Peer Quantum Cash System	Quantum teleportation, Quantum chain, Quantum blind signature, QKD, QRNG, Quantum computation
	[32]	Efficient Quantum Blockchain with a Consensus Mechanism QDPoS	QDPoS, Quantum voting(positive, negative, abstention), Weighted hypergraph state, Quantum state distribution center, Quantum signature, Trapped qubits, Consortium blockchain
	[103]	Quantum Bitcoin	Immediate local verification, One-coin mini-scheme, Subspace generator, Classical signature on coin, Quantum minting, Shards, Quantum channels
Quantum Blockchain Applications	[86]	A Blockchain Smart Contract Based on Light-Weighted Quantum Blind Signature	Quantum blind signature, Layered architecture, QKD, Quantum communication, Digitization of products and services, Quantum key
	[104]	A Simple Voting Protocol on Quantum Blockchain	Quantum blockchain adopted from section 4.2.1, CSQBC, QKD, Quantum channel, Byzantine Agreement, Classical channel, QSC, QHBA, Masked ballot, QKD

Category	Reference	Title	Technology
	[105]	Lottery and Auction on Quantum Blockchain	Pairwise quantum and classical channels, QKD, Quantum blockchain from section 4.2.1 and section 4.2.4, QBC, Flexible consensus, QHBA, Prize algorithm
	[14]	Decentralization using Quantum Blockchain: A Theoretical Analysis	θ - protocol, GHZ blockchain, QRNG, Double signature, QIA, Mutual quantum channels, Classical communication/storage, Quantum trapdoor function, Quantum public signature
	[106]	End to End Secure e-Voting Using Blockchain & Quantum Key Distribution	QKD, QBC, Classical blockchain, Quantum Digital signature, Voting machine

5.2.1. Strengths of Existing Research

Table 5: Quantum Blockchain Research Strengths

Category	Reference	Strengths
Hybrid Quantum Blockchains (QKD)	[5]	Novelty (QKD+Classical Blockchain), Experimenting (Fibre QKD, double spending), Theoretical Robustness (BFT, Informational Theoretical Security, Broadcast consensus), Possible integration with Q-internet, Scalability of QKD key rates.

Category	Reference	Strengths
	[89]	Quantum certificates and quantum protection, QHBA is not intensive, 50% dishonesty tolerance, Practical usage of Blockchain with qulogicoin and CSQBC, Implementable with current technology, Quantum security (QKD, QSDC).
	[92]	Unforgeable, transferable, and non-repudiable USS; Scalable QSYAC (quadratic on number of peers); Scripting language (declarative); Demonstrating the practical applicability with lottery; Practical with current tech.
	[93, 94]	Decentralization and blockchain, Dynamic allocation and functionalization of nodes (scalable), Quantum informational security, Crypto agility and future-proofing, New virtual quantum components (QSG, BG...), "Financion" to quantize transactions.
Hybrid Quantum Blockchains (Quantum Signature)	[82]	Efficient DPoSB, Quantum USS unforgeable, non-repudiable and secure against eavesdropping based on the computational indistinguishability of quantum states, Implementable with current tech (QKD, Quantum gates), Quantum information-theoretical security, Malicious behavior punishment.
	[95]	Energy efficiency in quantum mining, Innovation (PoE, Modems, Quantum servers), Thorough discussion of vulnerabilities, Detailed description of authentication mining and consensus, Forward-compatible in the quantum age, Experimental validation, Security of QSA, Trust only own devices.
Fully Quantum Blockchain	[96]	Clear conceptual framework about the chain and consensus over classical and quantum channels, Experimental feasibility of GHZ chain, Quantum tamper resistance of time entanglement.

Category	Reference	Strengths
	[97]	Novelty with hypergraph and many-bit classical to one-bit; Concrete math base and protocols for implementation; Experimental validation on IBM with high fidelity; Security analysis of tampering, external attacks, and dishonest peers; Clearly explains consensus.
	[101]	Novel cash system with teleportation (Double spending resistant), Quantum signature analogous to Bitcoin P2P, Block-less quantum chain for fast transactions, Quantum informational-theoretical security, Blind quantum computation allows transactions without compromising privacy.
	[32]	Quantum Voting-based consensus; Rigorous security analysis with tampering of blocks and forging of quantum signature; Efficient due to one-qubit blocks and simpler consensus; Comparison with other similar literature; Justified use of Quantum voting, quantum signatures, entanglement, and Hypergraph.
	[103]	Local verification of transactions saves time that typical consensus takes, Security analysis with counterfeiting and double-spending, Fully anonymous (no transaction records, hence no paper trail), No need to trust miners and the two-stage mining prevents malicious miner behavior, Immediate transaction validation without network interference (Scalability), Smaller Blockchain footprint (only minting records).

Category	Reference	Strengths
Quantum Blockchain Applications	[86]	Blind quantum signature for anonymity, privacy, and security of transactions; Suggested applications; Detailed security analysis of impersonation, forgery, and denial of signature; Independent of computational complexity; Efficient, lightweight, and scalable signature.
	[104]	Thorough security analysis, Use of established technology (QKD, BFT), Implementable with current tech.
	[105]	Not specified.
	[14]	Bridges the gap between quantum blockchain and identity management; QRNG and distributed verification tests which are practical in today's hybrid blockchain landscape; Decentralized identity management; Comprehensive theoretical analysis of Quantum states, quantum teleportation, quantum PKI, and GHZ; Entanglement for block data integrity and Quantum channels for anti-spoofing; Pseudonymization to prove identity info without revealing it.
	[106]	Not sufficiently developed or integrated with quantum technology to be analyzed.

5.2.2. Weaknesses in Literature

Table 6: Quantum Blockchain Research Weaknesses

Category	Reference	Weaknesses
Hybrid Quantum Blockchains (QKD)	[5]	Lack of Experimental Scale, Assumption of honest majority (2/3), Longer classical hash (no quantum hash), Data-intensive broadcast protocol, No detailed integration into Q-internet, No focus on anonymity.

Category	Reference	Weaknesses
	[89]	Lack of experimentation, lack of complexity or requirements of QHBA, Vulnerability of quantum storage, Ecosystem of quantum certificates not detailed, QHBA scalability not given.
	[92]	Assumption of honest majority (2/3), Vulnerability of quantum storage, Ecosystem of quantum certificates not detailed, Scalability of QSYAC and the Blockchain not discussed, Not focusing on deployment of quantum networks, Lacks experimentation.
	[93, 94]	CQKD computational and energy costs due to delegation, Lack of detail and clarity about the blockchain and consensus, No experimental validation of CQKD and community acceptance of delegation, Current lack of scalability of quantum infrastructure.
Hybrid Quantum Blockchains (Quantum Signature)	[82]	DPoSB complexity not discussed, Lack of experimentation, Does not discuss scalability of DPoSB or large dishonesty, Depends on a trusted node, Ecosystem of quantum certificates not detailed, Assumes honest majority (3/4).
	[95]	Largely theoretical, Extremely complex needing a network of quantum devices, Modified BFT not described, Quantum fiber network not scalable, An energy analysis more detailed with comparisons to popular blockchains, Difficult to realize in the near future due to complex quantum infrastructure.
Fully Quantum Blockchain	[96]	Purely conceptual and theoretical with no real-world application, Lack of details on consensus or malicious nodes, Lack of scalability discussions, Only two or a small string of bits per block, Lack of comprehensive security and privacy/confidentiality of transactions, Lack of quantum error correction.

Category	Reference	Weaknesses
	[97]	Miniature experimental scale, No discussion on transition from classical, No quantum error correction at scale, No discussion of distributed implementation or hardware requirements, Does not address scalability.
	[101]	Purely conceptual, No implementation/simulation to prove, No mention of Quantum Error Correction to achieve security and reliability, Scalability not discussed, Consensus not discussed, No security analysis against quantum adversaries.
	[32]	Practicality of quantum state distribution not discussed, Scalability of the voting that needs advanced quantum architecture not discussed, No focus on quantum error correction, One-time quantum signatures (cumbersome key management in the long term), No computational analysis of the voting protocol, Not discussed how QDPoS handles Byzantine fault, Lack of experimentation on real quantum hardware.
	[103]	Mentions a quantum signature but lacks details, Denominations of the coin not discussed, Lack of experimentation, Assumes majority is honest, Double spending mitigation lacks detail, Quantum error correction not discussed.
Quantum Blockchain Applications	[86]	Does not address practical security challenges (side-channel attacks or implementation vulnerabilities), Signature integration not described, Quantum Denial of Service (DoS) or quantum Man in The Middle (MiTM) attacks on the signature not focused on, Complexity of the multi-person signature not described, Lack of experimental validation, Scalability not described, Quantum error correction not described, Lack of practical implementation and scalability details.

Category	Reference	Weaknesses
	[104]	Assumes miners are honest, Although claimed for current technology; QBC, QSA, and other quantum tech question the current feasibility, Need to discuss technical challenges and resource needs, Need to discuss scalability with quantum technology.
	[105]	Not specified.
	[14]	Third-party authorities (issuers) to verify user attestations (Semi-centralized), Malicious issuers or collusion among issuers not discussed, Complexity or requirements of QBIF not covered, Lack of empirical validation, Only one transaction per GHZ block (Scalability), Broadcast limitations of entangled states lessen the scalability (lack of infrastructure), Quantum repeaters for long-range quantum communication are in research infancy, Network overhead due to interactive signatures, GHZ chain is theoretical and has decoherence, Primitive QRNG consensus, Unstable entanglement in time.
	[106]	Not sufficiently developed or integrated with quantum technology to be analyzed.

5.2.3. Research Gaps and Future Work per Work

Table 7: Quantum Blockchain Gaps per Work

Category	Reference	Gaps
Hybrid Quantum Blockchains (QKD)	[5]	Testing the protocol in larger, more complex networks; Increase dishonesty tolerance; Integrate quantum hash; Less data-intensive consensus for cases with dishonest or inactive nodes; Create anonymity and privacy; Quantum internet integration.

Category	Reference	Gaps
	[89]	Experiment with simulation or real-world implementation; Increase dishonesty tolerance($>$ 50%); Game-theoretic approaches to incentivize honest behavior; Quantum-secure storage solutions or quantum error correction techniques to protect quantum data/certificates; Complete an ecosystem for quantum certificates; Optimizing the QHBA protocol for large-scale; 2-layer architecture(quantum channels for high priority); Applications in quantum coin tossing, quantum oblivious transfer, or quantum multiparty computation; Make smarter and regulatable.
	[92]	Experimental validation of Logicontract and QSYAC; More resilient consensus to tolerate higher dishonesty with game-theory; Formal verification of logic-based smart contracts with a quantum framework; Logicontract (LC) application in quantum coin tossing, quantum oblivious transfer, or quantum multiparty computation; Optimize QSYAC for large scale; Standardized protocols for generating and verifying quantum certificates; Resources and runtime of smart contracts; Turing completeness of contract system.
	[93, 94]	Experimental validation and stress tests against quantum attacks, Adaptation for commercial relevance (Reduce complex quantum hardware needs), Address hybrid cyber-quantum attacks, How attacks like Grover's are resisted, MuRe-Qua and CQKD scalability not discussed, Quantum hash integration, Integrate into the current blockchain ecosystem.

Category	Reference	Gaps
Hybrid Quantum Blockchains (Quantum Signature)	[82]	Implement or simulate to evaluate scalability efficiency and security, Research on developing quantum internet/infrastructure, Quantum storage security, Remove key generator(decentralize signature by removing the trusted node), Quantum hash linking, Quantum privacy computing.
	[95]	Quantum error correction on servers and clients, Mentioned modified BFT could be detailed with steps.
Fully Quantum Blockchain	[96]	Perhaps attempt to combine with hypergraph; Large classical block to 2 or n-bit quantum block encoding (Scalability in general); Research on practical application in finance, government, etc, Quantum network consensus.
	[97]	Native consensus could be merged with classical-delegated-consensus, QKD / Quantum signature + Transaction syntax to make a niche application, Develop the bijective function.
	[101]	Quantum cloud for blind quantum management of coins(quantum states), Quantum error correction, Implement quantum blockchain to store remittance requests and quantum information by rigorous peer review(rather than only coins and transaction records), Create a minting process.
	[32]	Develop a bijective function, Develop/integrate a signature that can distribute unlimited copies of the key, Remove the quantum distribution center from QDPoS.
	[103]	Privacy-preserving techniques such as zero-knowledge proofs, Quantum blockchain implementation for forward compatibility, Integration with current blockchain finances.

Category	Reference	Gaps
Quantum Blockchain Applications	[86]	Verify quantum signatures on multiple blocks, Survey the impact of measurement error of quantum signatures on smart contracts, Asymmetric quantum keys in smart contracts, Quantum MITM and DoS.
	[104]	Modify for a scenario with dishonest miners, Side-channel attacks on QSC.
	[105]	Applying quantum blockchain to multi-party computation, Modify for a scenario with dishonest miners.
	[14]	Full decentralization removing centralized verification, Develop consensus for simultaneous communication, Increase block size, Make the chain more sustainable in the sense that the chain is unstable and difficulty in accessing.
	[106]	Not sufficiently developed or integrated with quantum technology to be analyzed.

6. Conclusion and Future Work

This section summarizes the observations of this literature review and attempts to emphasize on potential research directions.

6.1. Post-Quantum Blockchain

The quantum threat to cryptography is posed by Shor's and Grover's algorithms. Shor's algorithm is an immediate threat as a quantum adversary could break public-key cryptography and forge identities. Grover could quadratically accelerate the hash collision search or target nonce search in the context of a blockchain. The general stance in the community regarding Grover's attacks is to increase the hash size, i.e., enlarge the hash search space. Current research focuses on quantum hashing, which is irrelevant to post-quantum blockchains as they are still classical blockchains, and quantum hashing is a quantum technology. It is theoretically possible to keep increasing the hash size as quantum processors become more powerful; however, to have absolute security against Grover attacks, quantum hashing may have to be integrated into classical blockchains. The solution provided in the literature for classical blockchains against Shor's attacks is straightforward;

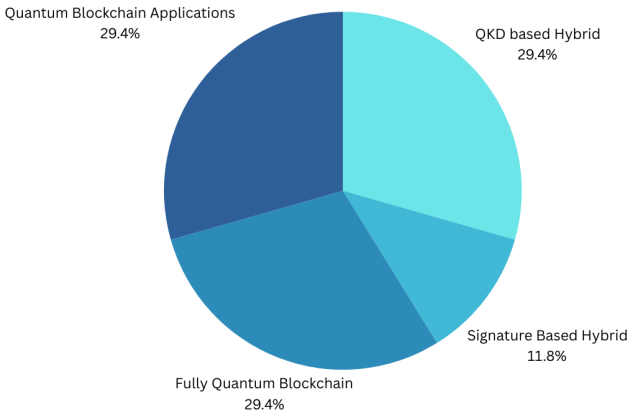

Figure 23: Distribution of Quantum Blockchain Literature

replace RSA, DSA, ECDSA, and Diffie-Hellman exchange with quantum-resistant classical public key encryption/signature schemes.

6.1.1. Future work

It would be an interesting outcome to see about integrating quantum hash functions, such as those given by Li et al.[36] and Hatanaka et al.[37], into a classical blockchain with post-quantum crypto primitives to have absolute security against Grover's attacks. In our opinion, solutions against Shor's attacks, i.e., post-quantum cryptography, could be deemed saturated. There are a plethora of cryptosystems that passed the fourth round in NIST's standardization, with more crypto primitives being proposed by researchers and cryptologists. Others focus on breaking those post-quantum crypto primitives with either classical or quantum approaches: for instance, Beullens[107] broke Rainbow. What can be contributed in this regard is to either formulate a new crypto primitive with higher efficiency and performance or refine existing NIST standardized encryption/signature schemes with smaller key sizes and ciphertext sizes.

6.2. Quantum Blockchain

We believe that there are more gaps than the actual work done in this area. Quantum computing is still in its infancy, whereas the full potential of blockchain is yet to be achieved. The combination of these two disruptive technologies is a novelty that has only seen a few years. The major trend in quantum blockchain is to focus on hybrid quantum blockchains and applications on them. That is, attach to a classical blockchain. One current

trend in fully quantum blockchain is to describe a quantum blockchain based on either GHZ states [96] or hypergraph states, emphasizing the novelty of the authors' devising on an aspect of the blockchain framework: authentication/signature, consensus, and communication. Blockchain applications researchers would propose financial applications (money, lottery, etc.) on a hybrid-quantum or quantum blockchain.

6.2.1. Future work

Future work per work is analyzed in section 5.2.3. Below, we have attempted to extract those research directions into categories of quantum blockchain in a more general form.

Table 8: General Future Work

Category	**General Future Work**
Hybrid Quantum Blockchains (QKD)	Test quantum blockchain protocols in larger, more complex networks, improve dishonesty tolerance (greater than 50%), integrate quantum hash, develop less data-intensive consensus mechanisms, and implement privacy and anonymity features. Explore quantum internet integration and hybrid cyber-quantum attacks.
Hybrid Quantum Blockchains (Quantum Signature)	Develop and implement quantum signature solutions for scalability, security, and decentralization. Integrate quantum hash linking and enhance quantum storage security. Investigate quantum error correction, and research quantum internet infrastructure for quantum signatures.
Fully Quantum Blockchain	Investigate hybrid consensus models, develop scalable applications in finance/government, and explore quantum error correction methods. Research the scalability of quantum blockchains and quantum minting processes. Investigate advanced quantum cloud management for secure storage and remittance. Work on the bijective function and quantum signature integration for large-scale use. Combine GHZ with Hypergraph

Category	General Future Work
Quantum Blockchain Applications	Explore full decentralization, develop advanced consensus protocols for quantum blockchain, and address security against attacks like MITM, DoS, and side-channel attacks. Investigate applications of quantum blockchain in multi-party computation, voting, lottery, and quantum certificates. Address the impacts of quantum signature measurement errors on smart contracts, and modify protocols for dishonest miners. Develop privacy-preserving techniques like zero-knowledge proofs.

We hope to conduct studies on quantum storage security in blockchain, quantum hash integration, quantum error correction in blockchain, and the conjunction of Hypergraphs and GHZ states in blockchain conceptualization.

References

[1] Muhammad Nasir Mumtaz Bhutta, Amir A. Khwaja, Adnan Nadeem, Hafiz Farooq Ahmad, Muhammad Khurram Khan, Moataz A. Hanif, Houbing Song, Majed Alshamari, Yue Cao, A survey on blockchain technology: Evolution, architecture and security, IEEE Access 9 (2021) 107619–107638, received March 2, 2021, Accepted March 19, 2021, Date of Publication April 13, 2021, Date of Current Version April 28, 2021. doi:10.1109/ACCESS.2021.3072849.

[2] R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (2) (1978) 120–126. doi:10.1145/359340.359342.

[3] N. I. of Standards, Technology, Digital signature standard (dss), https://csrc.nist.gov/pubs/fips/186-2/final, fIPS 186-2 (2000).

[4] D. Johnson, A. Menezes, S. Vanstone, The elliptic curve digital signature algorithm (ecdsa), International Journal of Information Security 1 (2001) 36–63. doi:10.1007/s102070100002.
URL https://doi.org/10.1007/s102070100002

[5] E. O. Kiktenko, et al., Quantum-secured blockchain, Quantum Science and Technology 3 (3) (2018) 035004. doi:10.1088/2058-9565/aabc6b.

[6] J. M. Jose, P. V, A survey on consensus algorithms in blockchain based on post quantum cryptosystems, in: 2022 5th International Conference on Computational Intelligence and Networks (CINE), IIT Kottayam, IEEE, Kottayam, India, 2022, p. X, iSBN: 978-1-6654-6465-9. doi:10.1109/CINE56307.2022.10037353.

[7] M. C. K. Khalilov, A. Levi, A survey on anonymity and privacy in bitcoin-like digital cash systems, IEEE Communications Surveys & Tutorials 20 (3) (2018) 2543–2585. doi:10.1109/COMST.2018.2818623.

[8] B. Lashkari, P. Musilek, A comprehensive review of blockchain consensus mechanisms, IEEE Access 9 (2021) 43620–43652. doi:10.1109/ACCESS.2021.3065880.

[9] S. Aggarwal, N. Kumar, Chapter twenty - attacks on blockchain, in: The Blockchain Technology for Secure and Smart Applications across Industry Verticals, Vol. 121 of Advances in Computers, Elsevier, 2021, pp. 399–410. doi:10.1016/bs.adcom.2020.08.020.
URL https://www.sciencedirect.com/science/article/pii/S0065245820300759

[10] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, National University of Singapore, Association for Computing Machinery, New York, NY, USA, 2016, p. 254–269. doi:10.1145/2976749.2978309.
URL https://doi.org/10.1145/2976749.2978309

[11] R. P. Feynman, Simulating physics with computers, International Journal of Theoretical Physics 21 (6) (1982) 467–488. doi:10.1007/BF02650179.
URL https://doi.org/10.1007/BF02650179

[12] M. Nakahara, T. Ohmi, Quantum Computing: From Linear Algebra to Physical Realizations, CRC Press, Boca Raton, FL, 2008. doi:10.1201/9781420087950.

[13] T. F. Rønnow, Z. Wang, J. Job, S. Boixo, S. V. Isakov, D. Wecker, J. M. Martinis, D. A. Lidar, M. Troyer, Defining and detecting quantum speedup, American Association for the Advancement of Science 345 (6195) (2014) 420–424.

[14] Z. Yang, T. Salman, R. Jain, R. D. Pietro, Decentralization using quantum blockchain: A theoretical analysis, IEEE Transactions on Quantum Engineering 3 (2022) 1–16. doi:10.1109/TQE.2022.3207111.

[15] D. Deutsch, R. Jozsa, Rapid solution of problems by quantum computation, Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences 439 (1907) (1992) 553–558. doi:10.1098/rspa.1992.0167.

[16] D. Simon, On the power of quantum computation, in: Proceedings 35th Annual Symposium on Foundations of Computer Science, Microsoft Corp., 1994, pp. 116–123. doi:10.1109/SFCS.1994.365701.

[17] Ethan Bernstein, Umesh Vazirani, Quantum complexity theory, SIAM Journal on Computing 26 (5) (1997) 1411–1473. doi:10.1137/S0097539796300921.

[18] C. Moore, A. Russell, The hidden subgroup problem – review and open problems, arXiv preprint arXiv:quant-ph/0411037 (2004). arXiv:quant-ph/0411037.
URL https://arxiv.org/abs/quant-ph/0411037

[19] Johanna Barzen, Frank Leymann, Post-quantum security: Origin, fundamentals, and adoption, in: Proceedings of the University of Stuttgart, University of Stuttgart, IAAS, Universitätsstr. 38, 70569 Stuttgart, Germany, 2023, p. XXX.
URL mailto:firstname.lastname@iaas.uni-stuttgart.de

[20] T. Scholten, C. Williams, D. Moody, M. Mosca, W. Hurley, W. J. Zeng, M. Troyer, J. Gambetta, Assessing the benefits and risks of quantum computers, NIST (7 2024).

[21] P. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: Proceedings of the 35th IEEE Symposium on Foundations of Computer Science, AT and T Bell Laboratories, 1994, pp. 124–134. doi:10.1109/SFCS.1994.365700.

[22] R. H. Preston, Applying grover's algorithm to hash functions: A software perspective, IEEE AccessThis work was supported by MITRE Independent Research and Development Program (2020).

[23] S. Jiang, K. A. Britt, A. J. McCaskey, T. S. Humble, S. Kais, Quantum annealing for prime factorization, Scientific Reports 8 (1) (2018) 17667. doi:10.1038/s41598-018-36058-z.
URL https://doi.org/10.1038/s41598-018-36058-z

[24] M. Maezawa, G. Fujii, M. Hidaka, K. Imafuku, K. Kikuchi, H. Koike, K. Makise, S. Nagasawa, H. Nakagawa, M. Ukibe, S. Kawabata, Toward practical-scale quantum annealing machine for prime factoring, Journal of the Physical Society of Japan 88 (6) (2019) 061012. doi:10.7566/jpsj.88.061012.
URL http://dx.doi.org/10.7566/JPSJ.88.061012

[25] B. Wang, F. Hu, H. Yao, C. Wang, Prime factorization algorithm based on parameter optimization of ising model, Scientific Reports 10 (1) (2020) 7106. doi:10.1038/s41598-020-62802-5.
URL https://doi.org/10.1038/s41598-020-62802-5

[26] M. Wroński, Practical solving of discrete logarithm problem over prime fields using quantum annealing, Cryptology ePrint Archive, Paper 2021/527 (2021).
URL https://eprint.iacr.org/2021/527

[27] A. Mahasinghe, Y. Jayasinghe, An initial step toward a quantum annealing approach to the discrete logarithm problem, Security and Privacy 5 (4) (2022) e234. doi:10.1002/spy2.234.
URL https://doi.org/10.1002/spy2.234

[28] Michał Wroński, Elżbieta Burek, Łukasz Dzierzkowski, Olgierd Żołnierczyk, Transformation of elliptic curve discrete logarithm problem to qubo using direct method in quantum annealing applications, Journal of Telecommunications and Information Technology 1 (2024) 75–82. doi:10.26636/jtit.2024.1.1463.

[29] J. Ding, G. Spallitta, R. Sebastiani, Effective prime factorization via quantum annealing by modular locally-structured embedding, Scientific Reports 14 (1) (2024) 3518. doi:10.1038/s41598-024-53708-7.
URL https://doi.org/10.1038/s41598-024-53708-7

[30] U. Skosana, M. Tame, Demonstration of shor's factoring algorithm for n

=

21 on ibm quantum processors, Scientific Reports 11 (1) (Aug. 2021). doi:10.1038/s41598-021-95973-w.
URL http://dx.doi.org/10.1038/s41598-021-95973-w

[31] A. Ekert, R. Jozsa, Quantum computation and shor's factoring algorithm, Reviews of Modern Physics 68 (3) (1996) 733–753. doi:10.1103/RevModPhys.68.733.

[32] Q. Li, J. Wu, J. Quan, J. Shi, S. Zhang, Efficient quantum blockchain with a consensus mechanism qdpos, IEEE Transactions on Information Forensics and Security 17 (2022) 1234–1245. doi:10.1109/TIFS.2022.1234567.

[33] Fredy Andres Aponte-Novoa, Ana Lucila Sandoval Orozco, Ricardo Villanueva-Polanco, Pedro Wightman, The 51% attack on blockchains: A mining behavior study, IEEE Access 9 (2021) 140549–140564. doi:10.1109/ACCESS.2021.3119291.

[34] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, SSRN Electronic Journal (2008). doi:10.2139/ssrn.3977007.
URL https://doi.org/10.2139/ssrn.3977007

[35] Q. Zhou, S. Lu, Hash function based on controlled alternate quantum walks with memory (september 2021), IEEE Transactions on Quantum Engineering 3 (2022) 1–10. doi:10.1109/TQE.2021.3130256.

[36] D. Li, Y.-G. Yang, J.-L. Bi, J.-B. Yuan, J. Xu, Controlled alternate quantum walks based quantum hash function, Scientific Reports 8 (1) (2018) 225. doi:10.1038/s41598-017-18566-6.
URL https://doi.org/10.1038/s41598-017-18566-6

[37] T. Hatanaka, R. Fushio, M. Watanabe, W. J. Munro, T. N. Ikeda, S. Sugiura, A quantum-resistant photonic hash function, arXiv preprint arXiv:2409.19932Version 1, submitted on 30 September 2024 (9 2024). arXiv:2409.19932.
URL https://api.semanticscholar.org/CorpusID:272987073

[38] Q. Zhou, X. Tang, S. Lu, H. Yang, A stable hash function based on parity-dependent quantum walks with memory, Hubei Key Laboratory of Distributed System SecuritySupported by the National Natural Science Foundation of China under Grant 62101197 and the China Postdoctoral Science Foundation under Grant 2021M691148. (8 2023).

[39] J. Hoffstein, J. Pipher, J. H. Silverman, Ntru: A ring-based public key cryptosystem, in: Proceedings of the 3rd International Symposium on Algorithmic Number Theory (ANTS), Vol. 1423 of Lecture Notes in Computer Science, Springer, Portland, OR, USA, 1998, pp. 267–288. doi:10.1007/BFb0054868.

[40] I. P. A. E. Pratama, A. Krisna, Post quantum cryptography: Comparison between rsa and mceliece, in: Proceedings of the International Conference on Information and Software Security (ICISS), IEEE, Jimbaran, Indonesia, 2022, p. XXX. doi:10.1109/ICISS55894.2022.9915232.

[41] R. J. McEliece, A public-key cryptosystem based on algebraic coding theory, Tech. rep., Deep Space Network Progress Report (2 1978).

[42] W. Lee, J.-S. No, Y.-S. Kim, Punctured reed–muller code-based mceliece cryptosystems, IET Communications 11 (10) (2017) 1543–1548. doi:10.1049/iet-com.2016.1301.

[43] A. Rostovtsev, A. Stolbunov, Public-key cryptosystem based on isogenies, Technical Report 2006/145, Cryptology ePrint Archive (2006). URL https://eprint.iacr.org/2006/145

[44] M. Research, Pqcrypto-sidh repository, GitHub, sIKEp434: matching ... AES128 (level 1) (20XX).

[45] J.F. Biasse, D. Jao, A. Sankar, A quantum algorithm for computing isogenies between supersingular elliptic curves, in: Lecture Notes in Computer Science, Vol. 8885, Springer, Cham, Switzerland, 2014, pp. 428–442.

[46] L. De Feo, D. Jao, J. Plût, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, Journal of Mathematical Cryptology 8 (3) (2014) 209–247.

[47] D. J. Bernstein, J. Buchmann, E. Dahmen, Post-Quantum Cryptography, Springer-Verlag, Berlin, Germany, 2009.

[48] J. Buchmann, E. Dahmen, A. Hülsing, XMSS: A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions, in: Proceedings of PQCrypto, Taipei, Taiwan, 2011, pp. 117–129.

[49] D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, Papachristodoulou, M. Schneider, P. Schwabe, Z. Wilcox-O'Hearn, SPHINCS: Practical Stateless Hash-Based Signatures, in: Proceedings of EUROCRYPT, Sofia, Bulgaria, 2015, pp. 368–397.

[50] K. Chalkias, J. Brown, M. Hearn, T. Lillehagen, I. Nitto, T. Schroeter, Blockchained post-quantum signatures, in: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics, IEEE, IEEE, R3, 2018, p. XXX.

[51] W. Castryck, T. Decru, An efficient key recovery attack on sidh, Cryptology ePrint Archive 2022 (2022) 975.
URL https://eprint.iacr.org/2022/975

[52] Google Security Blog, Experimenting with post-quantum cryptography, https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html, accessed: Nov. 2, 2019 (2016).

[53] A. H. Lone, R. Naaz, Demystifying cryptography behind blockchains and a vision for post-quantum blockchains, in: 2020 IEEE International Conference for Innovation in Technology (INOCON), IEEE, Bengaluru, India, 2020, p. XXX.

[54] N. Anhao, Bitcoin post-quantum, https://bitcoinpq.org/download/bitcoinpq-whitepaper-english.pdf, accessed: Jan. 29, 2023 (2018).

[55] Abelian, A quantum-resistant cryptocurrency balancing privacy and accountability, https://www.abelian.info/whitepaper.pdf, accessed: Jan. 29, 2023 (20XX).

[56] F. Shahid, A. Khan, S. U. R. Malik, K.-K. R. Choo, Wots-s: A quantum secure compact signature scheme for distributed ledger, Information Sciences 539 (2020) 229–249. doi:10.1016/j.ins.2020.05.024.

[57] C.-Y. Li, X.-B. Chen, Y.-L. Chen, Y.-Y. Hou, J. Li, A new lattice-based signature scheme in post-quantum blockchain network, State Key Laboratory of Networking and Switching Technology, Beijing University of Post and TelecommunicationsSupported by the National Natural Science Foundation of China Grant U1636106, Grant 61671087, and Grant 61170272, and other grants (2019).
URL yover100@163.com

[58] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, Y.-X. Yang, A secure cryptocurrency scheme based on post-quantum blockchain, State Key Laboratory of Networking and Switching Technology, Information Security Center, Beijing University of Posts and TelecommunicationsSupported by NSFC Grants 61671087, 61272514, 61170272, 61003287, the Major Science and Technology Support Program of Guizhou Province (20183001), the Fok Ying Tong Education Foundation (131067), and the Open Foundation of Guizhou Provincial Key Laboratory of Public Big Data (2017BDKFJJ007) (2023).
URL yover100@163.com

[59] R. Saha, G. Kumar, T. Devgun, W. J. Buchanan, R. Thomas, M. Alazab, T. Hoon-Kim, J. J. P. C. Rodrigues, A blockchain framework in post-quantum decentralization, IEEE Transactions on Services Computing 16 (1) (2023) 1–14, fellow, IEEE (Joel J. P. C. Rodrigues).

[60] C. Li, G. Xu, Y. Chen, H. Ahmad, J. Li, A new anti-quantum proxy blind signature for blockchain-enabled internet of things, Computers, Materials & Continua 61 (2) (2019) 711–726. doi:10.32604/cmc.2019.06279.
URL http://www.techscience.com/cmc/v61n2/33501

[61] L. Chao-Yang, C. Xiu-Bo, C. Yu-Ling, H. Yan-Yan, L. Jian, A new lattice-based signature scheme in post-quantum blockchain network, IEEE Access 7 (2019) 2026–2033. doi:10.1109/ACCESS.2018.2886554.

[62] W. A. A. Torres, R. Steinfeld, A. Sakzad, J. K. Liu, V. Kuchta, N. Bhattacharjee, M. H. Au, J. Cheng, Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (lattice ringct v1.0), in: Proc. ACISP, Wollongong, NSW, Australia, 2018, pp. 558–576.

[63] W. van der Linde, Post-quantum blockchain using one-time signature chains, in: Not Available, 2018, p. XXX.
URL https://api.semanticscholar.org/CorpusID:53419176

[64] W. Yin, Q. Wen, W. Li, H. Zhang, Z. Jin, An anti-quantum transaction authentication approach in blockchain, IEEE AccessState Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China (2020).

[65] X. Zheng, Research on blockchain smart contract technology based on resistance to quantum computing attacks, PLoS ONE 19 (5) (2024) e0302325, received: December 13, 2023; Accepted: April 2, 2024; Published: May 23, 2024. doi:10.1371/journal.pone.0302325.

[66] H. Yi, Secure social internet of things based on post-quantum blockchain, IEEE Transactions on Network Science and Engineering 9 (3) (2022) 950–957, date of Publication: 07 July 2021. doi:10.1109/TNSE.2021.3095192.

[67] S. Gao, D. Zheng, R. Guo, C. Jing, C. Hu, An anti-quantum e-voting protocol in blockchain with audit function, IEEE Access 7 (2019) 115304–115316. doi:10.1109/ACCESS.2019.2935895.

[68] H. Yu, W. Hui, Certificateless ring signature from ntru lattice for electronic voting, Journal of Information Security and Applications 75 (2023) 103496. doi:10.1016/j.jisa.2023.103496.

[69] H. Yi, Y. Li, M. Wang, Z. Yan, Z. Nie, An efficient blockchain consensus algorithm based on post-quantum threshold signature, Big Data Research 26 (2021) 100268. doi:10.1016/j.bdr.2021.100268.
URL https://doi.org/10.1016/j.bdr.2021.100268

[70] H. Kim, W. Kim, Y. Kang, H. Kim, H. Seo, Post-quantum delegated proof of luck for blockchain consensus algorithm, Applied Sciences

14 (18) (2024) 8394, submission received: 22 July 2024 / Revised: 13 September 2024 / Accepted: 16 September 2024 / Published: 18 September 2024. doi:10.3390/app14188394.

[71] J. Ding, A new proof of work for blockchain based on random multivariate quadratic equations, in: Applied Cryptography and Network Security Workshops, 2019, pp. 97–107. doi:10.1007/978-3-030-29729-9_5.

[72] J. Chen, W. Gan, M. Hu, C.-M. Chen, On the construction of a post-quantum blockchain for smart city, Journal of Information Security and Applications 58 (2021) 102780. doi:10.1016/j.jisa.2021.102780.

[73] Gorjan Alagic, Maxime Bros, Pierre Ciadoux, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Hamilton Silberg, Daniel Smith-Tone, Noah Waller, Status report on the first round of the additional digital signature schemes for the nist post-quantum cryptography standardization process, Tech. rep., National Institute of Standards and Technology, U.S. Department of Commerce, Information Technology Laboratory, nIST IR 8528 (10 2024).
URL https://doi.org/10.6028/NIST.IR.8528

[74] Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, Yi-Kai Liu, Status report on the third round of the nist post-quantum cryptography standardization process, Tech. rep., National Institute of Standards and Technology, U.S. Department of Commerce, Information Technology Laboratory, nIST Internal Report 8413. Former NIST employee Daniel Apon contributed while under contract with NIST (7 2022).
URL https://doi.org/10.6028/NIST.IR.8413

[75] T. M. Fernández-Caramés, P. Fraga-Lamas, Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks, IEEE Access 8 (2020) 21091–21116. doi:10.1109/ACCESS.2020.2968985.

[76] V. Gheorghiu, S. Gorbunov, M. Mosca, B. Munson, W. Paper, Quantum proofing the blockchain, Tech. rep.,

Blockchain Research Institute, University of Waterloo, Waterloo, ON, Canada, [Online]. Available: https://evolutionq.com/assets/mosca_quantum-proofing-the-blockchain_blockchain-research-institute.pdf (11 2017).

[77] M. Moizuddin, J. Winston, M. Qayyum, A comprehensive survey: Quantum cryptography, in: 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), 2017, pp. 98–102. doi:10.1109/Anti-Cybercrime.2017.7905271.

[78] Charles H. Bennett, Gilles Brassard, Quantum cryptography: Public key distribution and coin tossing, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (1984) 175–179.

[79] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, J.-W. Pan, Satellite-to-ground quantum key distribution, Nature 549 (2017) 43–47. doi:10.1038/nature23655.

[80] V. Padamvathi, B. V. Vardhan, A. Krishna, Quantum cryptography and quantum key distribution protocols: A survey, in: 2016 IEEE 6th International Conference on Advanced Computing (IACC), 2016, pp. 556–562. doi:10.1109/IACC.2016.109.

[81] Charles H. Bennett, Quantum cryptography using any two nonorthogonal states, Physical Review Letters 68 (21) (1992) 3121–3124. doi:10.1103/PhysRevLett.68.3121.

[82] W. Wang, Y. Yu, L. Du, Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm, Scientific Reports 12 (1) (2022) 8606. doi:10.1038/s41598-022-12412-0.
URL https://doi.org/10.1038/s41598-022-12412-0

[83] L. Yang, M. Liang, B. Li, L. Hu, D. Feng, Quantum public-key cryptosystems based on induced trapdoor one-way transformations, arXiv:

Quantum Physics (2010). arXiv:1012.5249, doi:10.48550/arXiv.1012.5249.

[84] M. Liang, L. Yang, Public-key encryption and authentication of quantum information, Science China Physics, Mechanics & Astronomy 55 (2012) 1618–1629. doi:10.1007/s11433-011-4806-y.

[85] D. Gottesman, I. Chuang, Quantum digital signatures (2001). arXiv:quant-ph/0105032.
URL https://arxiv.org/abs/quant-ph/0105032

[86] Maher Alharby, Amjad Aldweesh, Aad van Moorsel, Blockchain-based smart contracts: A systematic mapping study of academic research (2018), in: 2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB), 2018, pp. 1–6. doi:10.1109/ICCBB.2018.8756390.

[87] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, William K. Wootters, Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels, Phys. Rev. Lett. 70 (1993) 1895–1899. doi:10.1103/PhysRevLett.70.1895.
URL https://link.aps.org/doi/10.1103/PhysRevLett.70.1895

[88] M. Naor, Bit commitment using pseudorandomness, Journal of Cryptology 4 (2) (1991) 151–158. doi:10.1007/BF00196774.

[89] X. Sun, Q. Wang, P. Kulicki, X. Zhao, Quantum-enhanced logic-based blockchain i: Quantum honest-success byzantine agreement and qulogicoin (2018). arXiv:1805.06768.
URL https://arxiv.org/abs/1805.06768

[90] L. Hardy, A. Kent, Cheat sensitive quantum bit commitment, Physical Review Letters 92 (15) (4 2004). doi:10.1103/PhysRevLett.92.157901.

[91] X. Sun, Q. Wang, Bit commitment in categorical quantum mechanics, submitted to Quantum Information Processing (2018).

[92] x. sun, m. sopek, q. wang, p. kulicki, towards quantum-secured permissioned blockchain: signature, consensus, and logic, entropy 21 (9)

(2019). doi:10.3390/e21090887.
URL https://www.mdpi.com/1099-4300/21/9/887

[93] G. Iovane, Computational quantum key distribution (cqkd) on decentralized ledger and blockchain, Journal of Discrete Mathematical Sciences and Cryptography 24 (2021) 1021 – 1042.
URL https://api.semanticscholar.org/CorpusID:235542486

[94] G. Iovane, Murequa chain: Multiscale relativistic quantum blockchain, IEEE Access 9 (2021) 39827–39838. doi:10.1109/ACCESS.2021.3064297.

[95] A. J. Bennet and S. Daryanoosh, Energy efficient mining on a quantum-enabled blockchain using light, Ledger 4 (2019) 16. doi:10.5195/ledger.2019.143.

[96] d. rajan, m. visser, quantum blockchain using entanglement in time, quantum reports 1 (1) (2019) 3–11. doi:10.3390/quantum1010002.
URL https://www.mdpi.com/2624-960X/1/1/2

[97] Shreya Banerjee, Arghya Mukherjee, Prasanta K. Panigrahi, Quantum blockchain using weighted hypergraph states, Phys. Rev. Res. 2 (2020) 013322. doi:10.1103/PhysRevResearch.2.013322.
URL https://link.aps.org/doi/10.1103/PhysRevResearch.2.013322

[98] A. Banik, K. Supriya, H. El Ghor, B. Behera, P. K. Panigrahi, Demonstration of quantum blockchain using theta-protocol and different attacks on ibm qx, Quantum Reports 1 (1) (2020) 3–11. doi:10.3390/quantum1010002.

[99] C. Brukner, S. Taylor, S. Cheung, V. Vedral, Quantum entanglement in time (2004). arXiv:quant-ph/0402127.
URL https://arxiv.org/abs/quant-ph/0402127

[100] M. Rossi, M. Huber, D. Bruß, C. Macchiavello, Quantum hypergraph states, New Journal of Physics 15 (11) (2013) 113022. doi:10.1088/1367-2630/15/11/113022.
URL https://dx.doi.org/10.1088/1367-2630/15/11/113022

[101] K. Ikeda, qbitcoin: A peer-to-peer quantum cash system, in: K. Arai, S. Kapoor, R. Bhatia (Eds.), Intelligent Computing, Springer International Publishing, Cham, 2019, pp. 763–771.

[102] Q. Wang, C. Yu, F. Gao, H. Qi, Q. Wen, Self-tallying quantum anonymous voting, Physical Review A 94 (2) (2016). doi:10.1103/physreva.94.022333.
URL http://dx.doi.org/10.1103/PhysRevA.94.022333

[103] J. Jogenfors, Quantum bitcoin: An anonymous, distributed, and secure currency secured by the no-cloning theorem of quantum mechanics, in: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2019, pp. 245–252. doi:10.1109/BLOC.2019.8751473.

[104] X. Sun, Q. Wang, P. Kulicki, M. Sopek, A simple voting protocol on quantum blockchain, International Journal of Theoretical Physics 58 (1) (2019) 275–281. doi:10.1007/s10773-018-3929-6.
URL https://doi.org/10.1007/s10773-018-3929-6

[105] X. Sun, P. Kulicki, M. Sopek, Lottery and auction on quantum blockchain, Entropy 22 (12) (2020). doi:10.3390/e22121377.
URL https://www.mdpi.com/1099-4300/22/12/1377

[106] S. Gupta, A. Gupta, I. Y. Pandya, A. Bhatt, K. Mehta, End to end secure e-voting using blockchain & quantum key distribution, Materials Today: Proceedings 80 (2023) 3363–3370, sI:5 NANO 2021. doi:https://doi.org/10.1016/j.matpr.2021.07.254.
URL https://www.sciencedirect.com/science/article/pii/S2214785321051130

[107] Ward Beullens, Breaking rainbow takes a weekend on a laptop, in: Advances in Cryptology – CRYPTO 2022, Springer Nature Switzerland, Cham, 2022, pp. 464–479. doi:10.1007/978-3-031-15979-4_16.