A Survey on Quantum-safe Blockchain System

Swathi P.
pswathi@asu.edu
Arizona State University
Tempe, Arizona, USA

Dragan Boscovic
bdragan@asu.edu
Arizona State University
Tempe, Arizona, USA

ABSTRACT

Although blockchain technology is widely recognized for the near future, certain of its components are being challenged by another impending technology, quantum computing. Quantum-safe-blockchain is quickly becoming one of the essential future-proof blockchain designs. Quantum blockchain has a significantly greater scope than cryptocurrencies and cross-chain asset transactions. The majority of today's cryptography algorithms will be susceptible to quantum attacks. In this paper, a comprehensive literature review is performed by considering research questions regarding how quantum computing will affect the classical blockchain mechanism. The survey is completed by responding to the research questions and highlighting research gaps.

KEYWORDS

Quantum computers, Blockchain, Research, Crypto-currencies

ACM Reference Format:
Swathi P. and Dragan Boscovic. 2022. A Survey on Quantum-safe Blockchain System. In *Proceedings of Annual Computer Security Applications Conference (ACSAC).* ACM, Austin,TX, USA, 7 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Transaction systems in today's world are decentralized, transparent, and incorruptible. Instantaneous transactions and borderless ownership transfers are possible with digital money. Take bitcoin, for example, which disseminates the business of producing cash over the Internet. It employs computer algorithms to verify that funds are transferred safely from buyer to seller. Bitcoin's underlying technology, blockchain, provides transaction transparency and decentralized verification. A network of computers uses Bitcoin to maintain the collective public database [39]. All information about the transaction is locked when Bitcoin is uploaded to the blockchain. The transactions are verified and validated by bitcoin miners. If someone tries to tamper with the transaction, the node refuses to continue on the blockchain. A digital wallet is generated for each user on the user's node. Each wallet has a unique address, which serves as a network node's effective identification. A blockchain is a database that records all network transactions [16]. The validated transactions are uploaded to the blockchain as beads in a chain [26]. Each transaction is signed with confidential data called the private key, kept in the Bitcoin wallet. Every transaction is broadcast to all users. The network usually confirms it within the first 10 minutes, referred to as mining. In another way, mining is a distributed consensus method used to verify transactions awaiting inclusion on the blockchain.

The challenge of preserving the canonical blockchain state throughout the P2P network may be translated as a fault-tolerant state-machine replication problem in distributed systems. In other words, each consensus node keeps a local copy of the blockchain [4]. In the event of Byzantine/arbitrary failures, the consensus nodes are supposed to reach an agreement (i.e., consensus) on the unique shared view of the blockchain. Byzantine failures in blockchain networks lead defective nodes to behave in unpredictable ways((e.g., Sybil attacks and double-spending attacks) [52], node mistakes (e.g., unexpected blockchain fork owing to software incompatibility), and connection problems). A blockchain state transition occurs when a transaction is confirmed, and the sequence of blocks reflect the blockchain state [11].

The communication and trust between nodes in a distributed blockchain network must rely on digital signature technology, which primarily enables information identification, authenticity, and integrity verification. The encryption mechanism utilized in most blockchain digital signature technologies is Elliptic Curves Cryptography (ECC). The security of these methods is predicated on the idea that some mathematical issues are computationally hard. The proof-of-work mechanism is frequently employed for adding new data to the blockchain. The primary goal of this technique is to use a calculation to guess the nonce and solve the hash problem. On the other hand, the emergence of quantum computation may represent a threat to traditional blockchain technology [54]. Quantum computing is no longer simply a theoretical notion for businesses; it has a real-world application in creating economic value by effectively addressing complicated challenges [43], [14]. Several asymmetric keys and symmetric key cryptography techniques provide traditional security in IT systems. As an underlying cryptographic security provider, asymmetric key cryptographic algorithms such as ECDH (Elliptic Curve Diffie Hellman) algorithm, RSA (Rivest Shamir Adleman) encryption, EdDSA (Edwards-curve Digital Signature Algorithm), ECDSA (Elliptic Curve Digital Signature Algorithm), use complex problems in mathematics such as discrete logarithm problem, large integer factorization problem [[7], [51], [37]]. Symmetric key or shared key cryptographic methods employ block cipher techniques to produce a symmetric key for both encryption and decryption, such as DES (Data Encryption Standard), TDES (Triple DES), and AES (Advanced Encryption Standard) [10]. Some quantum algorithms can efficiently overcome the challenges associated with the encryption process, rendering the blockchain's digital signature insecure. If someone uses the Shor

ACSAC, December 2022, Austin, TX, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

algorithm [45] to extract a user's private key from a public key to sign a variety of fraudulent transactions, or if an attacker forges a user signature, the genuine users' assets and privacy will be lost. Remember that breaking Bitcoin's encryption and solving for private keys requires a 5,000-qubit quantum computer. Because quantum states are challenging to regulate, even the most powerful quantum computers can only handle 66 qubits right now [44].

The necessity for blockchain to withstand quantum algorithm attacks is critical. Many quantum-resistant public key cryptosystems have emerged due to the research work. The most competitive among them is the number of lattice-based public key cryptosystems. There currently needs to be a quantum method capable of solving the challenge of a lattice-based public key. Regev [42] described many lattice-based public key cryptosystem signatures. Quantum-resistant encryption gives optimism to blockchain users that it will be able to withstand quantum search algorithm attacks. On the other hand, Lattice cryptosystems often employ relatively large public keys and signatures. A decentralized, encrypted, and distributed database based on quantum computing and quantum information theory is what quantum blockchain is. The data will not be tampered with maliciously once it is captured on the quantum blockchain. The advancement of quantum computers and quantum information theory in recent years has drawn an increasing number of scholars to study quantum blockchain.

We seek to address four research questions, given the complexity of this study area:
RQ1: What is the current landscape concerning quantum safe blockchain, both in industry and academia?
RQ2: Are technological requirements for quantum safe blockchain currently satisfied?
RQ3: How does Quantum computing effect different layers of blockchain?
RQ4: Are there real use cases requiring quantum safe blockchain?

1.1 The Research Contributions are:

This article makes contributions as a conceptual model of knowledge on quantum safe blockchain:

- Introduce the quantum safe blockchain study topic by providing background information and emphasising definitions that are appropriate for both business and academics. The term "quantum safe blockchain" is defined, and several topologies and protocols are discussed.
- Discuss the effect of Quantum computing in different blockchain layers since each layer has various security requirements
- This work presents a comprehensive literature study in which we discover and explore quantum safe blockchain options. Our research is based on a variety of sources (e.g., peer-reviewed papers, whitepapers, blog posts, and technical reports), allowing us to gain a comprehensive grasp of each solution's present status and roadmap. This is our novel endeavour to provide the reader with high-quality information in this fast developing study area. This strategy enables us to receive current, dependable information, which is typically difficult to obtain.
- Identify and propose future study directions, opening the door for further systematic investigation in this field.

1.2 Organization

The rest of the paper is organized as follows: Section 2 gives background information on quantum, quantum safe blockchain, blockchain security, and how the quantum computing effects different layers of blockchain. Section 3 presents and discusses related literature reviews, while Section 4 discusses the research direction and finally Section 5 concludes the research work.

2 BACKGROUND

This section gives some background for understanding this survey before presenting the quantum secure blockchain, such as what is quantum computing, how it is expanding, and how it will affect blockchain security.

2.1 Quantum Computing

All bits of data in traditional computers are represented as either a 0 or a 1. This method is referred to as binary coding. Quantum computers, on the other hand, may do many calculations simultaneously due to the usage of quantum bits, also known as "qubits." Qubits may represent data in three states, that is, 0,1 and a quantum superposition of 0 and 1 [36]. Benioff [5] presented a two-order quantum system that may be utilized to imitate digital processing as early as the early 1980s. Quantum computing has become the primary form of mathematics over the past few years. Feynman [19] first suggested quantum computers in 1982. In terms of system architecture and performance, he proposed a fantastic computer using quantum physics. Bernstein and Vazirani finally realized the significance of Feynman's unique notion for cryptography twelve years later [8]. As a follow-up to Simon's study [47], Shor said [46] that the advent of quantum computers would endanger the very survival of public-key cryptography: currently complex instantiations of factoring and discrete logarithm issues would become cheap to solve. Grover also proposed the quantum database search method [23] in 1996. Shor et al. suggested a polynomial time quantum solution for factorization of large integer and discrete logarithm problems in 1997, putting the security of elliptic curve-based digital signatures at risk. D-wave has progressed from the first 16-bit quantum computer in 2007 to a 512-bit quantum computer, dramatically accelerating the development of quantum computers. Simultaneously, IBM in the United States has discovered a critical technology that may greatly expand the quantum number of quantum computers.

Quantum computers function by constructing and utilizing quantum superpositions to reduce the time it takes to solve (specific) computing tasks. Subgroup-finding algorithms and amplitude amplification are the two primary families of quantum algorithms relevant to the current subject. Shor's algorithm [45] best represents the first class of algorithms. This technique can factor big numbers and calculate the discrete logarithm in polynomial time. Amplitude amplification [[11],[54]] is the second type of method, and it is a generalization of Grover's search algorithm [23]. The significant distinction between quantum and traditional search algorithms is that quantum search algorithms are based on quantum mechanics. The best classical algorithm for unstructured search is the most straightforward brute-force strategy of guessing and testing across the search space in some random order. On the other hand, Grover's approach entails performing a series of quantum operations known as Grover iterations, followed by measurement, with each Grover iteration including two hashes. Unlike the usual brute-force technique, Grover's approach can only create a marked item after the measurement step.

The National Institute of Standards and Technology (NIST) has begun to demonstrate an interest in the standardization of quantum-resistant cryptography in recent years and has sponsored many relevant conferences. In 2015, the National Security Agency's Information Assurance Directorate announced the start of the shift to quantum-safe cryptography. PQCrypto and SAFEcrypto [11] are two post-quantum cryptography projects supported by the European Union. Using 32 ions, IonQ and the Duke Quantum Center have already accomplished quantum computing. It is conceivable to employ laser and photonic components built into a chip to minimize the size of the quantum computer. The MIT Lincoln Laboratory is conducting such research, having proven the use of silicon photonics for individual ion manipulation. By 2023, IonQ intends to leverage silicon photonics for ion qubit quantum computing [17].

2.2 Blockchain Security

Blockchain uses publicly recognized key cryptosystems to authenticate transactions using digitally identified signatures to ensure information exchange between participants. During the signature procedure, the signatory uses a private key to sign. The public key is exchanged openly to check that the signature is correct. Only the person who has a private key can create the algorithm. It is possible to encrypt it. Bitcoin employs ECDSA signatures to validate Koblitz signatures for private and public message signing [32]. Hash is also used to maintain credible records, i.e., to prevent evidence of tampering. As the validated data changes, the hash value varies accordingly. Quantum attacks are sensitive to transactions announced to the network, particularly in their signature scheme. If the transactions have yet to be integrated into a block but not broadcast to the network, then the transactions are prone to attack. A quantum attacker can find the private key by using the public key disclosed by the transaction sender. They can recreate the transaction with whatever output location they like. For example, Ethereum is built on an account-based system in which public keys are often reused. The attack method discovered may be used to target accounts that have previously disclosed transactions to the network while still holding some Ether tokens. A quantum attacker might falsify transactions in a user's name by creating a valid transaction signature by solving the public key to obtain the private key using Shor's algorithm. 317 ×106 physical qubits would be required to crack the encryption in one hour with a code cycle period of 1μs. It would take 1.9 ×109 physical qubits to break it in 10 minutes with the same code cycle time, but only 13 ×106 physical qubits to break it in a day [14].

Litecoin is vulnerable to quantum attacks since it shares its technical backbone with Bitcoin. Similar to Bitcoin, the most destructive attack strategy is to target transactions that have not yet been added to the blockchain. Bitcoin Gold, Bitcoin Core, and Bitcoin Cash are vulnerable due to commonalities in the Bitcoin cryptographic principles. Because it relies on the discrete logarithm issue, the signature system employed in Monero - EdDSA is vulnerable to quantum attacks. The anonymity of its users and the sums being exchanged provide Monero some resistance to quantum attacks. Although the Bulletproof protocol used by Monero to obfuscate transacted amounts is vulnerable to quantum attacks, an attacker would have to rely on chance to choose a transaction of considerable value [49]. Furthermore, owing to a recent upgrade in Monero's consensus protocol, where RandomX was added, it would be more resistant to quantum assaults attempting to use Grover's technique to accomplish a 51 percent attack. Quantum attacks are vulnerable to BEAM's signature system, Grin's signature scheme, and the Mimblewimble (a privacy and scalability upgrade deployed on the Litecoin network). Quantum attacks have the potential to capture network transactions as well as destroy anonymity from concealed transactions. The concealment of transaction and account values, like with Monero, reduces some of the motivation for a quantum attacker. The consensus mechanism and the signature system in ZCash are susceptible to quantum attacks. The most severe attack discovered against ZCash is a flaw in its zero-knowledge proof protocol ZK-SNARKS because this obfuscation approach necessitates a trusted setup and, as a result, the generation of a public key [12]. A quantum attacker who obtains the private key to this public parameter can produce tokens.

2.3 Blockchain Layers and Quantum computing

Each layer has various security requirements, thus we must do the study depending on these layers.

2.3.1 *Application Layer.*

The application layer is divided into the application layer and the execution layer. End users interact with the blockchain network through the application layer, which comprises intelligent contracts, underlying rules, and chain code. This sublayer includes the actual code and rules that are executed. A transaction is passed from the application to the execution layer. The execution layer handles transactions and ensures that the blockchain remains predictable. It accepts commands from the application layer [53]. A smart contract code should not be pulled down or updated once it has been placed on a blockchain, but with quantum computers, this may be achievable. Similarly, rather than making smart contracts more complicated inside the same technology, researchers should begin working towards quantum-resistant smart contracts immediately [18]. On top of the quantum-resistant blockchain platform, developers and companies can construct quantum-resistant smart contracts, DApps, DeFi solutions, NFTs, tokens, and the Metaverse in any programming language [28].

2.3.2 *Consensus Layer.*

The consensus layer is the most important layer for every blockchain. It establishes irreversible agreements between nodes in a distributed peer-to-peer network and maintains all nodes in the same phase. Consensus is in charge of verifying and arranging the blocks and ensuring that everyone agrees. With the assistance of quantum computers, it is simple to attack this layer. Attackers can look for hash collisions, which can then be utilized to modify blocks in a network without jeopardizing the blockchain's integrity. In addition, mining requires the search for a nonce, which will be extremely quick with quantum computers. An attacker may use this to rebuild the whole blockchain without being detected by the network.

2.3.3 Network Layer. The network layer guarantees that nodes discover other nodes, communicate, disseminate, and synchronize information, and are also in charge of global state propagation. A node can be either a light or a full node. The light nodes can send transactions and keep the blockchain's header, whereas full nodes are responsible for verification and validation, mining, and enforcing consensus rules. They are responsible for assuring the network's reliability. As a result, in the future, this layer will need to employ a quantum network.

2.3.4 Data Layer. Data is published to the blockchain network only when nodes establish consensus. Hash functions are used to aid in the identification of blocks and detect modifications made to the blocks. Transactions are digitally signed to protect the security and integrity of the data recorded on the blockchain. The blockchain uses asymmetric cryptography to safeguard information about the block. Private keys are utilized to sign a transaction, and anybody holding the public key may verify the signer. Digital signatures assure data integrity since the encrypted data is also signed. Each transaction in a block is hashed and organized as a Merkle tree. As a result, any tampering renders the signature invalid. Blockchain systems rely heavily on digital signatures to increase security. The difficulty of solving a mathematical puzzle, such as identifying the factors of big numbers, is used to generate these signatures. The data layer relies heavily on these algorithms, and once actual quantum computers are built, it will be simple to break them; hence, this layer is too sensitive to quantum attacks.

2.3.5 Hardware Layer. As distributed systems become widely accepted, peers may be connected and exchange data. This layer is in charge of generating virtual resources, including storage, networks, and servers. Nodes are a crucial component of this layer since they are physical devices that connect to the network and aid in blockchain consensus. Infrastructure security usually entails restricting or blocking node access. As a result, infrastructure improvements are required to fully implement a quantum secure blockchain.

3 RELATED LITERATURE REVIEW

Several experts have dedicated time and effort to securing Blockchain from a quantum computer assault in recent years. Two techniques are often used in this field of study: quantum-resistant Blockchain and quantum-secured Blockchain. The quantum-resistant computer blockchain system replaces the original signature with a quantum-resistant algorithm's digital signature. However, it is limited to theoretical studies and has little experience. The signed public key consumes a significant amount of block capacity. The problem of the long public key still needs to be solved. Several researchers are developing algorithms for digital signatures. Using the Bonsai Trees technology, Li devised a digital signature method. This algorithm can ensure its safety. It is, however, ineffective, and its viability must also be established [33]. Gao presented a double signature system for use on the blockchain [20]. However, the scheme's security is based only on the SIS assumption, which is unconvincing. Yin et al. expand a lattice space to many lattices based on Bonsai Tree [55]. This technique adds complexity to the signature. Moreover, the number of signatures generated by such systems is massive. Public key cryptosystems based on: hash function, error correction codes, lattice, and multivariable public key cryptosystems are the four dominant public key cryptosystems against quantum algorithms [23]. A lattice-based cryptosystem [16, 17] is now developed to solve two fundamental problems: small integer and learning error. Regev developed the LWE issue to make the lattice-based cryptography system considered verifiable security [42]. Ladner and Dwork used the single trap function on the lattice (GPV) to acquire the protiofate and used the protiofate sampling method to develop the public key encryption and signing schemes [45]. Post-quantum signatures are utilized to substitute classical signatures in quantum-resistant blockchain proposals [[11],[8]]. The authors of [54] and [8] propose a novel lattice-based signature system for securing blockchain transactions. Whereas [50] proposes a commit–delay–reveal protocol for safely transitioning from Bitcoin's existing signature system to a quantum-resistant signature scheme. These solutions are based on the (unproven) notion that quantum computers cannot tackle certain computational tasks effectively.

Many researchers have done much work in recent years to resist the quantum attack. Overall, a few views are quite promising in combating these challenges. Some classical methods will be used in quantum-resistant encryption to lessen the threat of a quantum computer attack. Shor's algorithm can readily solve several digital signature techniques on a sufficiently powerful quantum computer relying on the prime factorization of big integers and discrete logarithms. Hash-based cryptography, code-based cryptography, lattice-based cryptography, and multivariate-quadratic-equations cryptography are all good classical cryptographic systems expected to resist assaults from neither classical nor quantum devices [31]. The use of post-quantum digital signature techniques for signing transactions can improve the security of blockchains [3]. Such techniques are thought to resist quantum computer assaults [13]. This resilience, however, is based on untested assumptions. Furthermore, post-quantum digital signatures are computationally demanding, making them ineffective against attacks that use a quantum computer to control the network's hash rate. Other techniques for distributed ledger maintenance, such as Byzantine fault tolerance (BFT) replication and practical BFT replication, exist in addition to blockchains based on mining principles. All of the proposed alternatives involve using digital signatures, vulnerable to quantum computer attacks, or pairwise authenticated channels, at the very least. While the pairwise genuine channel assures that each message does not tamper in transit, it does not address the issue of transferability. Like the conventional blockchain, the quantum blockchain has several characteristics, such as decentralization. Quantum blockchain's major qualities are security and efficiency. Quantum blockchain security must be guaranteed. Quantum secure direct communication (QSDC) [30], or quantum key distribution (QKD) [[21],[6]] are two methods for ensuring communication security between nodes. As a result, network authentication is assured by quantum physics features.

Table 1: Summary of research work done

Literature	Concepts discussed
Benioff et.al[5]	Presented a two-order quantum system that may be utilised to imitate digital processing.
Feynman et.al[19]	Suggested quantum computers.
Bernstein et.al[8]	It showed that there can be advantages in using a quantum computer as a computational tool for more complex problems.
Simon et.al[47]	This work described an anticipated polynomial-time quantum computer algorithm that differentiates between two relatively reasonable classes of polynomial-time computable functions.
Shor et.al[45]	Introduced a polynomial-time quantum computer algorithm for integer factorization. And also explained advent of quantum computers would endanger the very survival of public-key cryptography.
Grover et.al[23]	Proposed the quantum database search method.
[3]	The topic of whether graph isomorphism has an efficient solution on the quantum Turing computer sparked the research discussed in this paper.
Brassard et.al[9]	This paper combined the ideas from Grover's and Shor's quantum algorithms to perform amplitude estimation.
Regev et.al[42]	The use of Fourier analysis on lattices as an integrated aspect of a lattice-based construction was presented in this study. They design tools that describe specific Gaussian distributions around lattice points in a beautiful way.
Perlner et.al[41]	A study of some of the public key cryptography algorithms that are considered to be resistant to quantum computing-based assaults, despite the fact that they are not currently in general usage.
Manuel et.al[54]	Detailed explanation of quantum computers.
Gerhardt et.al[21]	The first full-field implementation of a comprehensive assault on a functioning QKD connection is demonstrated in this work.
Pan et.al[40]	A novel efficient lattice-based public-key cryptosystem with a knapsack has been presented that can withstand Pan and Deng's attack.
Kuo et.al[31]	The Shortest Vector Problem (SVP), which involves finding the shortest vector in a given lattice, is at the heart of the lattice-based cryptosystem. The authors re-design the implementation technique based on the prior results in order to boost GPU performance.
Bennet et.al[6]	A system for coin-tossing based on the exchange of quantum messages was presented, which is safe against typical types of cheating, even by an opponent with infinite computational capacity.
Mettler et.al[35]	This research tries to show how blockchain technology may have a variety of effects, purposes, and potentials.
Zhang et.al[56]	The authors devised a technique based on smart contracts and encrypted currencies to facilitate the exchange of smart property and paid data. Finally, they devised two experiments to test these IoT E-business model assumptions.
Ding et.al[1]	Post quantum cryptography was introduced.
Chen et.al[13]	The authors propose an enhanced P2P file system architecture based on IPFS and Blockchain based on IPFS's properties. They introduced the role of content service providers to address the high-throughput challenge for individual users in IPFS.
Ali et.al[2]	This study proposes a decentralised access paradigm for IoT data, based on a network architecture for IoT and blockchains that is a modular consortium architecture.
Kiktenko et.al[30]	This study provides a solution to the quantum era blockchain difficulty and describes the experimental implementation of a quantum-safe blockchain platform that uses quantum key distribution across an urban fibre network for information-theoretically secure authentication.
Kamil et.al[24]	The authors developed a system supports both single- and multi-threaded execution and enables Gaussian sampling for trapdoor lattices with prime moduli. They test the implementation by putting it to the test in the GPV hash-and-sign digital signature technique as a benchmark.
Diana et.al[34]	A complete review of post-quantum cryptography was provided. In contrast to previous well-known studies that emphasise the need of developing post-quantum public-key cryptographic algorithms.
Singhal et.al[48]	Reviewed grover's algorithm.
[20]	A signature system based on the lattice problem is proposed in this study. The authors create secret keys using the lattice basis delegation process and sign messages using the preimage sampling approach.
Yin et.al[55]	This study introduces a blockchain-based anti-quantum transaction authentication mechanism. To assure the unpredictability and security of the master private key, each transaction signature employs a lattice space.
Cui et.al[15]	The advancement of quantum computation revealed flaws in the emerging blockchain technology in this article. The authors demonstrate that the future of blockchain technology is constantly threatened.
Kearney et.al[29]	The authors look at the major blockchain-based cryptocurrencies in use , such as Bitcoin, Ethereum, Litecoin, and ZCash, to see how vulnerable they are to quantum assaults.
Hattenbach et.al[25]	This document examines different signature methods that are currently being standardised by the National Institute of Standards and Technology (NIST). Authors analysed which currently available implementations are more suitable for IoT use-cases after discussing the fundamental foundation for why certain schemes are different in some respects compared to others.
Hugh et.al[14]	This technical report gives the summary of IBM Quantum Summit 2021,in which, IBM unveiled its new 127-quantum bit (qubit) 'Eagle' processor.
Sankar et.al[44]	This technical report says "Startups in quantum computing are popular, but it's uncertain if they'll be able to generate anything practical in the coming years".
Mohit et.al[38]	This study examines a variant of RSA cryptography known as Symmetric-RSA, which appears to be equally helpful for a variety of cryptographic applications like encryption, digital signatures, and so on.

In a traditional blockchain, the digital signature may also verify that the owner has the bitcoin. However, as previously stated, traditional encryption techniques employed in digital signatures, such as RSA, may become insecure in the face of quantum computer assaults. The quantum digital signature mechanism can be utilized in quantum blockchain to tackle this problem [22]. As a result, the quantum blockchain possesses quantum security properties. Quantum computers might not be able to attack the quantum blockchain. Fast transaction processing speed is another feature of the blockchain using quantum technology. The POW based on Analog Hamiltonian Optimizers can reduce transaction time, as previously stated. This effort will have a significant impact on the greater adoption of bitcoin and other blockchain applications. Furthermore, adopting the Grover algorithm to the broader blockchain can boost the mining process' efficiency. In reality, everything is a two-edged sword. The parties with access to universal quantum computers have an unfair edge in obtaining mining rewards until they generally become available. In their paper, Erik [27] explained that quantum computers cannot yet compromise blockchain security since they are not yet developed enough. Researchers have been preparing potential countermeasures since they first realized the harm quantum computing posed. Therefore, although quantum computing is still in its infancy, numerous interesting ideas have already been put forth. These remedies include quick fixes like post-quantum cryptography and other suggestions to strengthen the blockchain's defenses against quantum computers. While these safeguards may be applied with existing technology, neither total security nor long-term defenses like quantum cryptography and quantum blockchains are provided. It is impossible to predict how long it will take or whether we will ever have quantum computers that could break the blockchain because the most recent generation of quantum computers cannot run Grover's or Shor's algorithm. By that time, quantum technology may already be so extensively used that no one without a quantum computer can take control of the network, while classical hardware may be far.

Overall, as compared to traditional blockchain, quantum blockchain's performance advantage is mostly due to its security and efficiency. For better understanding the literature is summarized in Table 1.

4 RESEARCH DIRECTION

Quantum blockchain has a bright future in the realm of quantum digital money. Although many academics have proposed quantum money, quantum blockchain can still improve these quantum currency systems. Quantum Bitcoin, for example, employs a traditional blockchain, much like the Bitcoin protocol. As a result, we may consider replacing the conventional blockchain in Quantum Bitcoin with a quantum blockchain. Furthermore, the method of employing quantum blockchain to create a new, safer, and more efficient money system merits further investigation. However, the usage of quantum blockchain is not restricted to quantum digital money; any technology that relies on distributed storage and consensus procedures might benefit from it. As a result, research on using quantum blockchain for other jobs such as electronic voting, online auctions, and multiparty lotteries may be conducted. Extending the scope of the experiment is a viable idea. Furthermore, suppose additional quantum blockchain protocols, such as quantum-enhanced logic-based blockchain, can be tested experimentally. In that case, the viability of these protocols may be compared using the findings of these tests. This research might be used to build a true quantum blockchain platform.

5 CONCLUSIONS

Blockchain innovations have developed quickly in the current decade. With the expanding reception of blockchain innovation, the quantity of clients has consistently expanded. This article discusses weak points in blockchain technology revealed by the emergence of quantum computation. Although quantum computing is still in its early stages, it holds the potential of extremely powerful computers. Both blockchain and quantum computation are active research topics, and we anticipate they will evolve in the next decade. Quantum blockchain will have a wide variety of applications and research avenues in the future due to its properties of quicker processing speed and safer transactions based on quantum mechanics. Blockchain is a developing technology that is considered the cornerstone of web 3.0. As demonstrated by the advancement of quantum computers, quantum computing is currently more than just a theoretical concept. As highlighted in the paper, quantum computers pose serious risks to the classical blockchain protection mechanism. According to our literature analysis, work must be done at every layer of the blockchain, not just one, to keep it stable even with quantum computers. By doing that, we can create a secure blockchain with the advent of an attack.

REFERENCES

[1] *Post-Quantum Cryptography : 11th International Conference, PQCrypto 2020, Paris, France, April 15-17, 2020, Proceedings / edited by Jintai Ding, Jean-Pierre Tillich.* Security and Cryptology ; 12100. Springer International Publishing, Cham, 2020.

[2] Ali, M. S., Dolui, K., and Antonelli, F. Iot data privacy via blockchains and ipfs. In *Proceedings of the Seventh International Conference on the Internet of Things* (New York, NY, USA, 2017), IoT '17, Association for Computing Machinery.

[3] Beals, R. Quantum computation of fourier transforms over symmetric groups. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing* (New York, NY, USA, 1997), STOC '97, Association for Computing Machinery, p. 48–53.

[4] Ben, E., Brousmiche, K.-L., Levard, H., and Thea, E. Blockchain for enterprise: Overview, opportunities and challenges.

[5] Benioff, P. Quantum mechanical hamiltonian models of turing machines. *Journal of Statistical Physics 29* (1982), 515–546.

[6] Bennett, C. H., and Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science 560* (2014), 7–11. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[7] Bernstein, D. J., Josefsson, S., Lange, T., Schwabe, P., and Yang, B.-Y. Eddsa for more curves. *IACR Cryptol. ePrint Arch. 2015* (2015), 677.

[8] Bernstein, E., and Vazirani, U. Quantum complexity theory. In *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing* (New York, NY, USA, 1993), STOC '93, Association for Computing Machinery, p. 11–20.

[9] Brassard, G., Høyer, P., Mosca, M., and Tapp, A. Quantum amplitude amplification and estimation, 2002.

[10] Burke, J., McDonald, J., and Austin, T. Architectural support for fast symmetric-key cryptography. In *Proceedings of the Ninth International Conference on Architectural Support for Programming Languages and Operating Systems* (New York, NY, USA, 2000), ASPLOS IX, Association for Computing Machinery, p. 178–189.

[11] Cachin, C., and Vukolić, M. Blockchain consensus protocols in the wild, 2017.

[12] Chen, T., Lu, H., Kunpittaya, T., and Luo, A. A review of zk-snarks, 2022.

[13] Chen, Y., Li, H., Li, K., and Zhang, J. An improved p2p file system scheme based on ipfs and blockchain. *2017 IEEE International Conference on Big Data (Big Data)* (2017), 2652–2657.

[14] Collins, H. Ibm unveils breakthrough 127-qubit quantum processor.

[15] Cui, W., Dou, T., and Yan, S. Threats and opportunities: Blockchain meets quantum computation. In *2020 39th Chinese Control Conference (CCC)* (2020),

pp. 5822–5824.

[16] Dinh, T., Liu, R., Zhang, M., Chen, G., Ooi, B., and Wang, J. Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering PP* (08 2017).

[17] Emilio, M. D. P. Current status and next in quantum computing. *EE Times Europe* (07 2022).

[18] Faridi, A., Masood, F., Shamsan, A., Luqman, M., and Salmony, M. Blockchain in the quantum world, 02 2022.

[19] Feynman, R. P. Simulating physics with computers. *International Journal of Theoretical Physics 21*, 6 (1982), 467–488.

[20] Gao, Y.-L., Chen, X.-B., Chen, Y.-L., Sun, Y., Niu, X.-X., and Yang, Y.-X. A secure cryptocurrency scheme based on post-quantum blockchain. *IEEE Access 6* (2018), 27205–27213.

[21] Gerhardt, I., Liu, Q., Lamas-Linares, A., Skaar, J., Kurtsiefer, C., Ma, Z., and Makarov, V. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Communications 2* (06 2011), 349.

[22] Gottesman, D., and Chuang, I. Quantum digital signatures.

[23] Grover, L. K. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing* (New York, NY, USA, 1996), STOC '96, Association for Computing Machinery, p. 212–219.

[24] Gur, K. D., Polyakov, Y., Rohloff, K., Ryan, G. W., and Savas, E. Implementation and evaluation of improved gaussian sampling for lattice trapdoors. In *Proceedings of the 6th Workshop on Encrypted Computing and Applied Homomorphic Cryptography* (New York, NY, USA, 2018), WAHC '18, Association for Computing Machinery, p. 61–71.

[25] Hattenbach, H. Quantum-resistant digital signatures schemes for low-power iot, 2021.

[26] Kamilaris, A., Fonts, A., and Prenafeta Boldú, F. The rise of blockchain technology in agriculture and food supply chains.

[27] Kappert, N., Karger, E., and Kureljusic, M. Quantum computing - the impending end for the blockchain?

[28] Katy. Qanplatform, the world's first quantum-resistant eth-compatible l1 coming to aibc dubai.

[29] Kearney, J. J., and Perez-Delgado, C. A. Vulnerability of blockchain technologies to quantum attacks. *Array 10* (2021), 100065.

[30] Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., Lvovsky, A. I., and Fedorov, A. K. Quantum-secured blockchain. *Quantum Science and Technology 3*, 3 (may 2018), 035004.

[31] Kuo, P.-C., and Cheng, C.-M. Lattice-based cryptanalysis — how to estimate the security parameter of lattice-based cryptosystem. In *2014 IEEE International Conference on Consumer Electronics - Taiwan* (2014), pp. 53–54.

[32] Lange, T. Koblitz curve cryptosystems. *Finite Fields and Their Applications 11*, 2 (2005), 200–229.

[33] Li, C.-Y., Chen, X.-B., Chen, Y.-L., Hou, Y.-Y., and Li, J. A new lattice-based signature scheme in post-quantum blockchain network. *IEEE Access 7* (2019), 2026–2033.

[34] Maimut, D., and Simion, E. Post-quantum cryptography and a (qu)bit more.

[35] Mettler, M. M. Blockchain technology in healthcare: The revolution starts here. *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)* (2016), 1–3.

[36] Microsoft. The qubit in quantum computing.

[37] Miller, V. S. Use of elliptic curves in cryptography. In *Advances in Cryptology — CRYPTO '85 Proceedings* (Berlin, Heidelberg, 1986), H. C. Williams, Ed., Springer Berlin Heidelberg, pp. 417–426.

[38] Mohit, P., and Biswas, G. P. Modification of traditional rsa into symmetric-rsa cryptosystems. *Int. J. Bus. Data Commun. Netw. 13*, 1 (jan 2017), 66–73.

[39] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Cryptography Mailing list at https://metzdowd.com* (03 2009).

[40] Pan, Y., Deng, Y., Jiang, Y., and Tu, Z. A new lattice-based public-key cryptosystem mixed with a knapsack. vol. 7092, pp. 126–137.

[41] Perlner, R. A., and Cooper, D. A. Quantum resistant public key cryptography: a survey. In *IDtrust '09* (2009).

[42] Regev, O. New lattice-based cryptographic constructions. *J. ACM 51*, 6 (nov 2004), 899–942.

[43] Savage, N. Google's quantum computer achieves chemistry milestone.

[44] Sharma, S. D. Quantum computing has a hype problem. Tech. rep., 03 2022.

[45] Shor, P. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994), pp. 124–134.

[46] Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing 26*, 5 (1997), 1484–1509.

[47] Simon, D. On the power of quantum computation. In *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994), pp. 116–123.

[48] Singhal, A., and Chatterjee, A. Grover's algorithm.

[49] Sovbetov, Y. Factors influencing cryptocurrency prices: Evidence from bitcoin, ethereum, dash, litcoin, and monero. *Journal of Economics and Financial Analysis 2* (02 2018), 1–27.

[50] Stewart, I., Ilie, D., Zamyatin, A., Werner, S., Torshizi, M., and Knottenbelt, W. Committing to quantum resistance: A slow defence for bitcoin against a fast quantum computing attack. *Royal Society Open Science 5* (06 2018), 180410.

[51] Sutter, G., Deschamps, J.-P., and Imaña, J. Efficient elliptic curve point multiplication using digit-serial binary field operations. *Industrial Electronics, IEEE Transactions on 60* (01 2013), 217–225.

[52] Swathi, P., Modi, C., and Patel, D. Preventing sybil attack in blockchain using distributed behavior monitoring of miners. pp. 1–6.

[53] Szabo, N. Smart contracts : Building blocks for digital markets.

[54] Vogel, M. Quantum computation and quantum information, by m.a. nielsen and i.l. chuang. *Contemporary Physics 52*, 6 (2011), 604–605.

[55] Yin, W., Wen, Q., Li, W., Zhang, H., and Jin, Z. An anti-quantum transaction authentication approach in blockchain. *IEEE Access 6* (2018), 5393–5401.

[56] Zhang, Y., and Wen, J. The iot electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications 10* (2017), 983–994.