Received: 12 September 2024 | Revised: 7 November 2024 | Accepted: 25 November 2024

DOI: 10.1049/qtc2.12119

The Institution of Engineering and Technology WILEY

REVIEW

Quantum blockchain: Trends, technologies, and future directions

Manjula Gandhi S[1] | Chaitrali Mulay[2] | Karthiganesh Durai[2] | G. Murali[3] | Jafar Ali Ibrahim Syed Masood[4] | V. Vijayarajan[4] | Kumar Gautam[5,6] | N. S. Kalyan Chakravarthy[7] | S. Suresh Kumar[7] | Saurabh Agarwal[8] | Murali S[4] | Vijayasherly V[4] | David Asirvatham[9] | Sarfraz Brohi[10] | Chandru Vignesh C[4] | Anbuchelian S[11]

[1]Department of Computing, Coimbatore Institute of Technology, Coimbatore, Tamil Nadu, India

[2]KwantumG Research Labs Pvt Ltd, Bengaluru, India

[3]Department of Mechanical Engineering, Koneru Lakshmaiah Education Foundation, Vijayawada, Andhra Pradesh, India

[4]School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India

[5]Quantum Computing Lab, Quantum Research and Centre of Excellence, New Delhi, Delhi, India

[6]Department of Quantum Technology, Vivekananda Institute of Professional Studies-Technical Campus, Pitampura, India

[7]Centre for Data Science, AI&ML, QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India

[8]Department of Information and Communication Engineering, Yeungnam University, Gyeongsan, Republic of Korea

[9]Faculty of Innovation and Technology, Taylor's University, Subang Jaya, Selangor, Malaysia

[10]School of Computing and Creative Technologies, University of the West of England, Bristol, UK

[11]Ramanujan Computing Centre, Anna University, Chennai, Tamil Nadu, India

Correspondence

Jafar Ali Ibrahim Syed Masood.
Email: jafarali.s@vit.ac.in

Funding information

VIT University

Abstract

Blockchain technology is a highly developed database system that shares information within a business web. It stores details in blocks connected chronologically, ensuring information integrity through consensus mechanisms that prevent unauthorised alterations. This decentralised system removes the need for a believable mediator, mitigating vulnerabilities and enhancing transaction security. Blockchain's application spans the energy, finance, media, entertainment, and retail sectors. However, classical blockchain faces threats from quantum computing advancements, necessitating the development of quantum blockchain technology. Quantum blockchain, leveraging quantum computation and information theory, offers enhanced security and immutability. In this paper, different mathematical foundations, practical implementations and effectiveness of lattice-based cryptography in securing blockchain applications are discussed. Analysis of how the cryptographic techniques can protect blockchain systems against quantum attacks is being done by using mathematical formulations and examples. Quantum computing strengthens blockchain security with advanced encryption and authentication, which is critical for safeguarding diverse sectors from evolving cyber threats. Further study on quantum-resistant design is necessary if blockchain networks are to be robust and intact in the face of future technological developments.

KEYWORDS

quantum computing, quantum gates, quantum information

1 | INTRODUCTION

The advent of quantum computing poses a significant threat to security models under classical realm. Cryptographic techniques such as prime factorisation (RSA) and discrete logarithms are being used for years together for encryption. Quantum algorithms such as Shor's and Grover's are able to break these cryptographic systems. This opens up the need for quantum safe cryptographic techniques. This paper gives a brief overview of how Shor's algorithm can break classical cryptographic schemes, giving insights about quantum threat to cryptography, and also stresses on the need for post-quantum cryptographic methods in blockchain, that is, the importance of quantum resistant cryptography. It also focuses on lattice based cryptography, by introducing its importance for blockchain quantum resistance. Thus, the integrity of blockchain systems needs to be preserved in the post-quantum era. The urgency to protect the critical systems from vulnerabilities introduced by quantum computing is the key driver behind research in quantum blockchain. The next subsection discusses the fundamental concepts behind quantum computing, details about qubit, superposition states, entangled states and GHZ states.

1.1 | Background

- **Qubit**

Classical bits can be either 0 or 1, but a qubit can be zero and one or anywhere between zero and one at a particular time. Qubits [1] obey the quantum mechanical laws, letting us process information differently. Qubits are represented using 2D vectors as given in Equation (1.1).

$$\Big|q>=\cos\frac{\theta}{2}\Big|0>+e^{i\phi}\sin\frac{\theta}{2}\Big|1>, \qquad (1.1)$$

θ *and* ϕ are real numbers

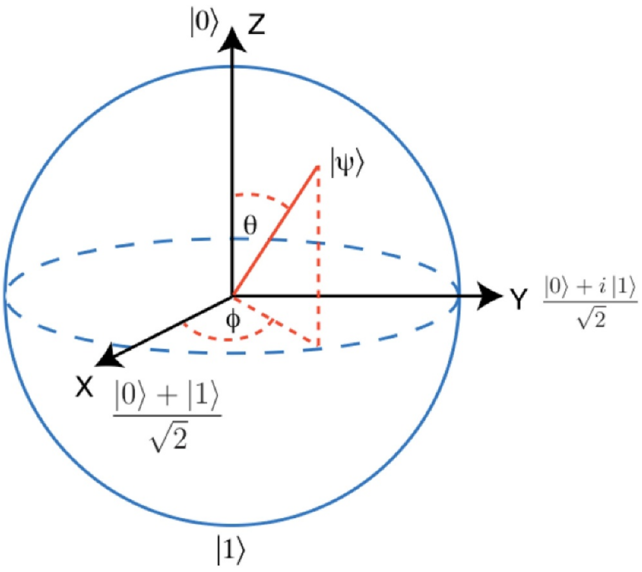
Figure 1 shows the three computational bases: X, Y, and Z. The Z Gate eigenstates {|0>, |1>} construct the Z-basis. The X Gate eigenstates {|+>, |–>} shape the X-basis as given in Equation (1.2). The Y Gate eigenstates {|+i>, |–i>} construct the Y-basis, as shown in Equation (1.3).

$$\Big|+>=\frac{1}{\sqrt{2}}(|0>+|1>)\ \ and\ \ \Big|->=\frac{1}{\sqrt{2}}(|0>-|1>) \qquad (1.2)$$

$$\Big|+i>=\frac{1}{\sqrt{2}}(|0>+i|1>)\ \ and\ \ \Big|-i>=\frac{1}{\sqrt{2}}(|0>-i|1>) \qquad (1.3)$$

- **Superposition**

A qubit characterised by simultaneous existence in zero and one is called a superposition. A superposition in various output representations of IBM's Qiskit [2] for the state |+>, which is observed when applying the Hadamard gate on qubit value |0>, is shown in Figure 2. The various output representations of a superposition state are Histogram, QSphere, State Vector, and BlochSphere in Qiskit as shown in Figures 2a,2b, 2c, and 2d, respectively.



|0⟩
Z
|ψ⟩
θ
ϕ
Y
$\frac{|0\rangle+i|1\rangle}{\sqrt{2}}$
X
$\frac{|0\rangle+|1\rangle}{\sqrt{2}}$
|1⟩

FIGURE 1 Computational basis.

- **Entangled States**

"Spooky action at a distance" was the description for entanglement by Einstein, defined as an effect at the subatomic level involving non-classical associations amongst spatially alienated quantum machines. A Quantum circuit to generate entanglement [3] is given in Figure 3, and the truth table is depicted in Table 1.

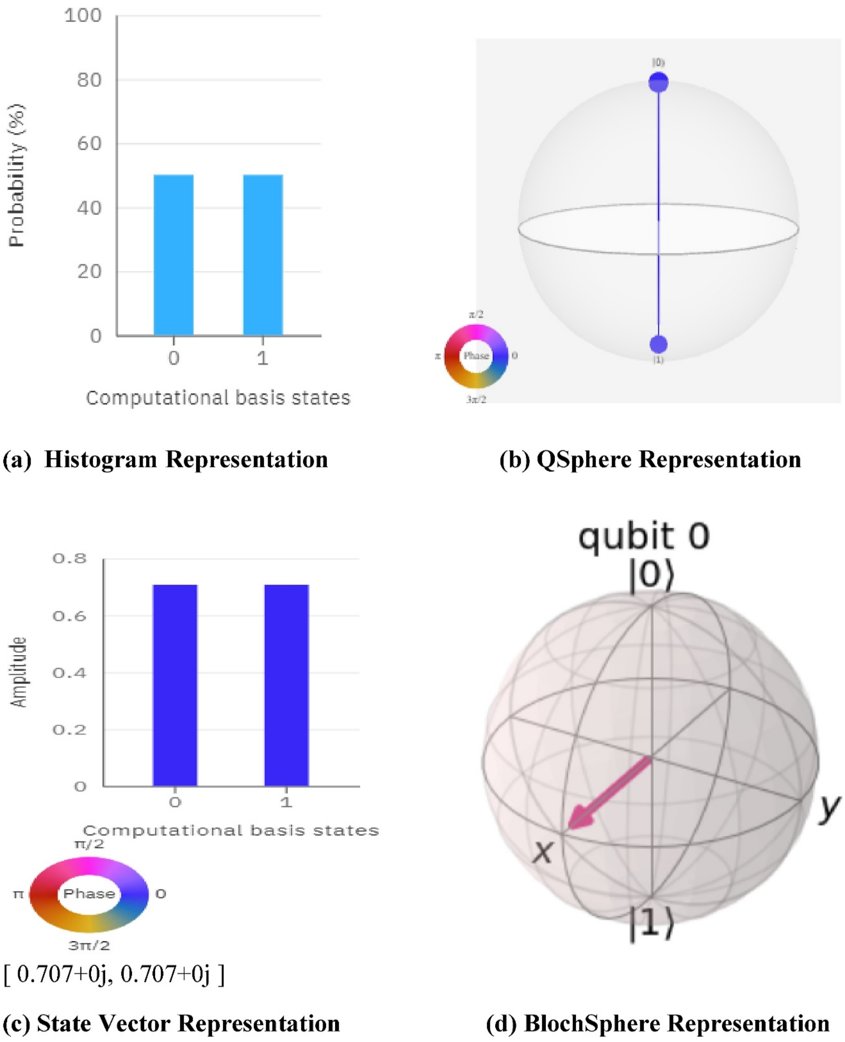
When the input is |10>, the output of the entangled state in QSphere and state vector representation is shown in Figures 4a and b.

- **GHZ State**

Figure 5 gives the Qiskit code to generate the Greenberger–Horne–Zeilinger (GHZ) state using three qubits, and the respective circuit is shown in Figure 6. The measurement relationships of the GHZ state [4] are tougher than an association produced by a classical machine.

1.2 | Limitations of classical blockchain technology

- Scalability—Blockchain networks, especially those using proof of work consensus mechanisms like bitcoin, struggle when the number of users is more. Each transaction must be validated by all nodes in the network, which leads to bottlenecks and slow transaction processing times. This lack of scalability makes its use difficult in high demand applications.



(a) Histogram Representation

(b) QSphere Representation

[0.707+0j, 0.707+0j]

(c) State Vector Representation

(d) BlochSphere Representation

FIGURE 2 Representation of a superposition state in various forms.

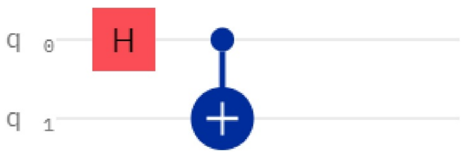


FIGURE 3 Entanglement circuit.

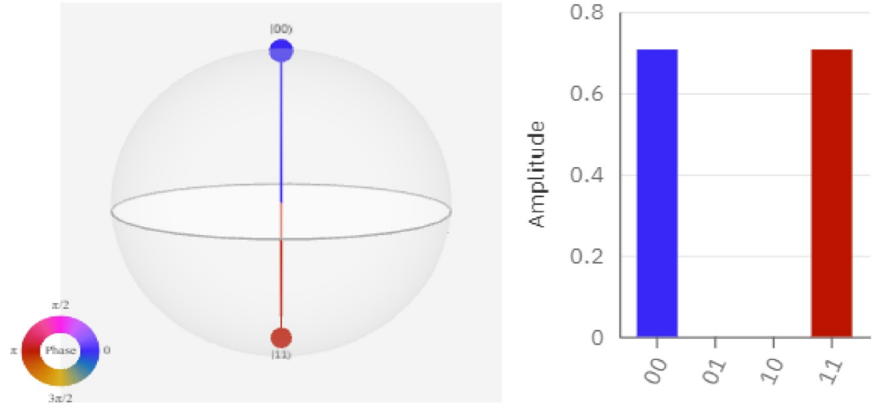
TABLE 1 Truth table for entanglement.

In	Out
00	$\frac{1}{\sqrt{2}}(\|00> +\|11>)$
01	$\frac{1}{\sqrt{2}}(\|01> +\|10>)$
10	$\frac{1}{\sqrt{2}}(\|00> -\|11>)$
11	$\frac{1}{\sqrt{2}}(\|01> -\|10>)$

- Energy efficiency—Example of high energy consumption is bitcoin mining, as it consumes vast amounts of computational resources and electricity. This energy inefficiency is a significant barrier to the widespread adoption of blockchain.
- Transaction speed—Classical blockchains suffer from slow transaction speeds. The decentralised nature of blockchain makes the transactions to be validated and agreed upon by all nodes in the network; this takes minutes or even hours for the transaction to complete.
- Quantum vulnerability—Vulnerability to quantum attacks is an important factor in the security of classical systems. Systems like RSA and elliptic curve cryptography are based on classical problems like prime factorisation. However, quantum algorithms like Shor's can break the encryption methods and can be effectively used more efficiently.
- Decentralisation and latency—Decentralisation introduces latency issues, which makes it difficult to handle large transactions.

1.3 | Need of quantum blockchain technology

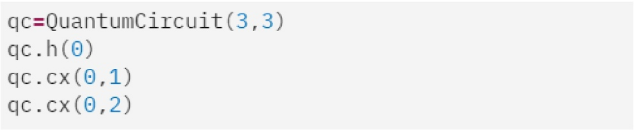
Classical cryptographic methods such as RSA (Rivest–Shamir–Adleman) and ECC (elliptic curve cryptography) are becoming obsolete, leading to a surge in interest in quantum safe



a) QSphere Representation

b) State Vector Representation

FIGURE 4 Entanglement output when input is |10>.



```
qc=QuantumCircuit(3,3)
qc.h(0)
qc.cx(0,1)
qc.cx(0,2)
```

FIGURE 5 Qiskit code to generate a three-qubit GHZ state.

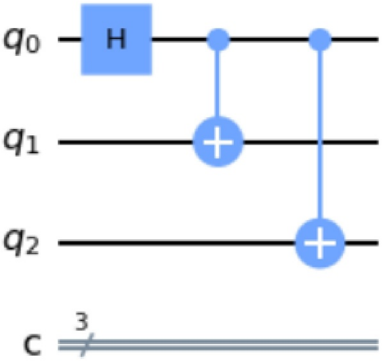


FIGURE 6 Three-qubit GHZ state.

cryptography. Methods such as lattice-based cryptography and hash based methods, which can withstand quantum attacks, are being used in various areas such as quantum finance, healthcare and communication domains. Major financial institutions are investing in research and development in the field of quantum computing. Sectors such as healthcare are using blockchain for decentralised and secure data sharing to protect their financial operations against cyber threats. Quantum communication can enhance the scalability and speed of blockchain systems. Quantum parallelism opens up the door for more efficient consensus mechanisms and faster transaction validations. Several countries such as USA, UK, and China are funding research in quantum computing and quantum safe cryptography.

This study is essential for ensuring future security of industries that are increasingly adopting blockchain technologies. Quantum blockchain, by incorporating quantum resistant algorithms, can prevent quantum-based cyberattacks. It provides an opportunity to enhance blockchain's performance. Quantum computing offers significant improvements in processing power. Also, this study is important for fostering innovation for quantum cryptography. It paves the way for developing new quantum safe cryptographic methods to be implemented for many industries.

Seeing through these challenges, quantum blockchain technology can be a genuine solution. Quantum blockchain leverages the characteristics of quantum mechanics, including the superposition of states and quantum entanglement, to introduce a paradigm shift in security natively immune to computational requirements projected for quantum computers. The research review is an exploratory study of quantum blockchain trends, technologies and future directions that will address the current lack pointed out above to bridge classical insecurity vulnerabilities towards their post-quantum secure solutions.

Indeed, blockchain technology has significantly transformed the storage and sharing of data across a decentralised network, enhancing its security. From banking to healthcare, it possesses a resilient structure for transactions that cannot be altered. However, introducing new algorithms, such as Grover's search algorithm and Shor's factoring algorithm by quantum computing, presents a severe threat to established blockchain systems, potentially undermining the cryptology principles that safeguard these networks.

The data is sequentially ordered, and the chain cannot be discarded or altered without agreement from the system. Therefore, this apparatus enables us to prepare an invariable or unchangeable record book for monitoring systems, payments, financial records, and other affairs. It has intrinsic processes that refrain from unofficial negotiations. An authentic agent has to look into and authenticate transactions to safeguard from future legal complications. The authentication of this mediator complicates the transaction and creates vulnerabilities. Blockchain overcomes such problems by presenting a segregated, secured system to show the deals. It produces one account book each for the customer and the merchant. Both sides must authenticate all deals and are spontaneously upgraded in both their records immediately. The characteristics as mentioned earlier have driven the adoption of blockchain technology in diverse industries like energy, banking, media, entertainment, and retail. The susceptibility of classical blockchain technology to quantum assaults is attributed to the progress made in quantum computing, notably by the development of Shor's factoring algorithm in 1992 and Grover's search algorithm in 1994.

1.4 | Technical terms

- **Quantum resistant**

Also known as **quantum-safe** or **post-quantum**, it refers to cryptographic algorithms or systems that are designed to withstand attacks from quantum computers. Quantum computers, once fully developed, are expected to be much more powerful than classical computers, especially in solving certain mathematical problems that are fundamental to current cryptographic methods (like RSA and ECC). Quantum-resistant algorithms are those that cannot be efficiently broken by quantum algorithms such as Shor's algorithm (which could break RSA) or Grover's algorithm (which reduces the security of symmetric cryptography). These post-quantum cryptographic methods are designed to secure data even in a future where quantum computers are operational.

- **Post-quantum cryptography**

Post-quantum cryptography refers to cryptographic algorithms and protocols that are designed to be secure against attacks by quantum computers. Unlike traditional cryptographic methods such as RSA, ECC (elliptic curve cryptography), and others, which could be broken by quantum algorithms like Shor's algorithm, post-quantum cryptographic algorithms are built to remain secure even in the presence of powerful quantum computers. These algorithms rely on mathematical problems that are believed to be hard for both classical and quantum computers to solve. Common approaches include lattice-based cryptography, hash-based cryptography, code-based cryptography, and multivariate quadratic equations. The goal of post-quantum cryptography is to ensure long-term security in a future where quantum computing is viable.

- **Quantum Secure**

Quantum secure, also known as **quantum-safe**, refers to cryptographic systems, protocols, or algorithms that are designed to remain secure even against attacks from quantum computers. These systems are resilient to the computational power of quantum algorithms, like Shor's or Grover's algorithms, which can break many of the cryptographic methods currently in use (e.g. RSA and ECC). Quantum secure algorithms are part of post-quantum cryptography, and they aim to protect data from being decrypted or compromised, even in a future where quantum computing is widely available. The term encompasses both symmetric and asymmetric cryptographic systems that resist quantum attacks.

1.5 | Advantages of quantum blockchain

Quantum blockchain offers several advantages over classical blockchain systems, particularly by integrating the principles of quantum computing and quantum cryptography. Here are the key benefits:

a. Quantum Resistance

Quantum blockchain systems use quantum-resistant cryptography to defend against the computational power of quantum computers. Classical blockchains, which rely on RSA or ECC, are vulnerable to quantum algorithms like Shor's. Quantum blockchain addresses this vulnerability by utilising cryptographic protocols based on quantum-safe algorithms such as lattice-based, hash-based, or multivariate polynomial cryptography. This makes them immune to quantum-based attacks.

b. Enhanced Security through Quantum Cryptography

Quantum blockchain can utilise quantum key distribution (QKD), which offers theoretically unbreakable encryption. QKD enables two parties to generate a shared random secret key, which is secured using the principles of quantum mechanics. Any attempt to eavesdrop on this communication would alter the quantum state, alerting the participants to the intrusion. This ensures a highly secure transaction environment.

c. Faster Consensus Mechanisms

Quantum computing can speed up some consensus algorithms, such as proof of stake (PoS) or even quantum byzantine fault tolerance (QBFT). Quantum algorithms can process and verify blocks more quickly than classical computers, potentially solving scalability and latency issues that plague classical blockchains. This could increase transaction throughput, making blockchain more efficient and scalable for real-world applications.

d. Improved Efficiency

Quantum computing excels at solving complex optimisation problems efficiently. Quantum blockchains could leverage this to optimise resource management in terms of energy use, reducing the computational and energy costs associated with consensus mechanisms like proof of work (PoW). This could make quantum blockchains greener and more sustainable.

e. Stronger Privacy and Anonymity

Using quantum cryptographic techniques, quantum blockchains can offer enhanced privacy. Quantum-based encryption can ensure that only intended recipients can access transaction data, and quantum techniques such as quantum zero-knowledge proofs could enable more secure and private transactions without revealing sensitive information.

f. Enhanced Interoperability

Quantum algorithms may help resolve current challenges in blockchain interoperability. By providing more efficient algorithms for cross-chain communication and transaction verification, quantum blockchains could facilitate smoother interactions between different blockchain networks.

g. Quantum Randomness for Enhanced Security

Classical blockchains rely on pseudo-random number generation (PRNG), which can potentially be exploited by powerful adversaries. Quantum blockchain systems can generate truly random numbers using quantum phenomena, which greatly enhances the security of cryptographic keys and transaction protocols.

h. Potential for New Applications

Quantum blockchain could open the door for applications in fields that require high-level security and computational power, such as secure voting systems, supply chain management, healthcare data sharing, and IoT (Internet of Things) networks. These applications would benefit from the enhanced security and processing power quantum blockchain provides.

In summary, quantum blockchain presents a future-proof solution to the vulnerabilities of classical blockchain systems while enhancing security, scalability, and efficiency. The combination of quantum computing and blockchain technologies creates opportunities for more advanced applications in a wide range of fields. This initiates the necessity for developing quantum blockchain technology. It might be conceptualised as a dispersed, scattered, encoded database based on quantum information theory and quantum computation. Unauthorised parties cannot access information encoded in the quantum blockchain technology. This article surveys various aspects related to blockchain technology, such as futuristic security aspects, blockchain-based security schemes, authentication protocols, AI for quantum blockchain, and applications of quantum blockchain.

2 | QUANTUM CRYPTOGRAPHIC TECHNIQUES

Current blockchain technologies rely on computational difficulty assumptions and are susceptible to cyberattacks. Quantum informatics offers potential solutions for enhancing blockchain security. Security and privacy measures must be implemented across diverse sectors, including online transactions, digital banking transfers, cryptocurrency, and tax payments. The looming advent of quantum computing has been pushing for more work and developing post-quantum cryptographic algorithms.

2.1 | Lattice-based cryptography

Lattices are discrete sets of vectors in n dimensional space. Quantum computers will not be able to achieve exponential advantageous speedup against lattice-based cryptographic [5] systems because the problem underlying these cryptosystems is also believed to be hard for quantum algorithms, that is, it belongs to a particular class of problems (LWE). The lattice problems in this cryptographic approach are assumed to be very difficult in quantum and classical computers. Lattice-based cryptography is a general structure that was recently shown to be helpful in building cryptographic fundamentals such as encryption, digital signatures, and identity-based encryption. There is a wide variety of potential applications in quantum blockchain, especially when creating secure digital signatures and key exchange protocols resistant to quantum decryption.

A lattice in an n dimensional space is a regular arrangement of points. It can be defined as the set of all points generated by integer linear combinations of a set of linearly independent vectors that span the space. Let $v_1,v_2,\ldots,v_n$ be linearly independent vectors in R^n. The lattice L generated by these vectors is the set of all points as given in Equation (2.1).

$$L = \left\{ \sum_{i=1}^{n} z_i v_i \mid z_i \in \mathbb{Z} \right\} \tag{2.1}$$

Lattice problems are highly significant in applications related to post-quantum cryptography such as mathematics and cryptography. Lattice-based cryptography is a robust and secure post-quantum method capable of being deployed in public key cryptosystems. A lattice-based aggregate signature technique with security predicated on the difficulty of the ring learning with errors (Ring-LWE) problem was presented by Bagchi et al. [6]. One such core framework for the same is being implemented in IoDah (Internet of Drones on a high authority blockchain), which suits well with various security measures and provides transparent store operations using technology like blockchain. The proposed mechanism incorporates improved security attributes, robustness against quantum assault vectors, and efficiency advantage over conventional contemporary approaches. The proof of concept (an experiment and blockchain simulations) demonstrates this proposed scheme's feasibility and practical applicability to real-world drone applications.

2.2 | Shortest vector problem

- Most fundamental and well-studied lattice problems. It asks for the shortest non-zero vector in a lattice, measured in terms of its Euclidean length.
- Given a lattice L generated by a set of basis vectors, the goal is to find a lattice vector $v \: \varepsilon \: L \setminus \{0\}$ such that it satisfies Equation (2.2).

$$\|v\| = \min\{\|u\| \mid u \in L, u \neq 0\} \tag{2.2}$$

- SVP is a NP hard problem and is computationally difficult to solve.
- It plays a key role in the cryptanalysis of lattice-based cryptographic schemes and forms the basis of hardness assumptions in cryptography.

2.2.1 | Learning with errors (LWE) problem

- It can be viewed as a generalisation of noisy linear systems and is believed to be hard even for quantum computers.
- Given a random matrix $A \in \mathbb{Z}_q^{m\times n}$, a secret vector s and an error vector e with small entries (modulo q), the goal is to recover the vector s given the "noisy" linear equations.
- b = As + e (mod q)
- b is the vector of observations, challenge is to find s, even if the system is perturbed by error vector e.
- The hardness of LWE forms the basis for many cryptographic schemes, such as homomorphic encryption, digital signatures etc.
- Different types of LWE are search LWE, decision LWE etc.

2.2.2 | Steps involved in LWE-based public key encryption

Step 1: Key generation

Parameters—choose a prime modulus q, lattice dimensions n and m, and an error distribution χ.

Selection of secret key and public key.

Step 2: Encryption

Computation of the ciphertext is done using Equation (2.3)

$$\text{Ciphertext} = (c_1, c_2) = \left(A^T x \;(\text{mod } q), b^T x + \lfloor q/2 \rfloor \;\mu(\text{mod } q)\right) \tag{2.3}$$

Step 3: Decryption

Given the cipher text, the decryption process uses the secret key s to recover the message using (2.4)

$$c_2 - c_1^T s \;(\text{mod} \quad q) \tag{2.4}$$

2.2.3 | Practical use of LWE in public key encryption

- LWE is a hard problem in lattice-based cryptography that forms the foundation of many cryptographic systems, particularly in post-quantum cryptography.
- Public key encryption schemes based on LWE are believed to be secure even against quantum adversaries.

2.3 | *N*th Degree Truncated Polynomial Ring (NTRU) encryption

NTRU (*N*th degree truncated polynomial ring) is a lattice-based public key cryptosystem, relying on the hardness of certain problems in the arithmetic of polynomials, specifically within truncated polynomial rings. It is considered as one of the key candidates for post-quantum cryptography because of its resistance to quantum attacks. Key features of NTRU are

1) Lattice-based: NTRU belongs to the family of lattice-based cryptosystems.
2) Polynomial ring arithmetic: Encryption and decryption are based on operations in a polynomial ring.
3) Efficiency: Very efficient compared to other lattice-based cryptosystems.
4) Post-quantum security: Believed to be secure even against quantum computers.
5) The core operations in NTRU encryptions rely on polynomial arithmetic in a specific ring.
6) Polynomial ring: Ring of polynomials modulo $X^N - 1$.
7) Modulus q: Operates with coefficients of polynomials reduced modulo, a small integer q, which controls the size of the polynomial coefficients.
8) The ring structure is given in Equation (2.5).

$$R_q = \mathbb{Z}_q\,[X]/\left(X^N - 1\right) \tag{2.5}$$

2.4 | Performance metrics

Dilithium is a lattice-based digital signature scheme designed to provide post-quantum security. It is based on the LWE and LWR problems, both of which are computationally hard. Practical applications of this scheme include

1) Secure communication and data integrity
2) Secure software distribution

3) Blockchain and cryptocurrencies
4) Post-quantum TLS (transport layer security)
5) IoT (Internet of Things) security
6) Government and military communications

Kyber is a lattice-based key encapsulation mechanism that can be used for key exchange or public key encryption. It is based on the LWR (learning with rounding) problem, a variant of the LWE problem. Key features of Kyber are

1) Security—based on the hardness of lattice problems such as LWR, known to be hard even for quantum computers.
2) Efficiency—highly efficient in terms of computational cost, bandwidth usage etc.
3) Post-quantum resistance—considered secure against both classical and quantum adversaries.
4) Procedure for Kyber key exchange—key generation, encapsulation, and decapsulation.

Comparison of encryption and decryption times for lattice-based cryptographic schemes are shown in Table 2.

Real world blockchain trade-offs are compared and shown in Table 3.

3 | BLOCKCHAIN AND QUANTUM-RESISTANT ALGORITHMS

Quantum-resistant algorithms are fundamental to quantum blockchain technology, providing strong security measures against the enormous computational capabilities of quantum computers. Our systems will be more secure when present encryption techniques are combined with quantum-resistant cryptographic algorithms than when used alone. While these algorithms have promise, they each excel in different areas and may struggle when applied to problems in the real world.

TABLE 2 Comparison of encryption and decryption time.

Scheme	Encryption time	Decryption time
RSA—2048	1.5 ms	16 ms
RSA—3072	3 ms	25 ms
ECC—256	0.5 ms	1 ms
Dilithium	0.3–0.5 ms	0.8–1.2 ms
Kyber	0.2–0.6 ms	0.4–1.0 ms

Quantum-resistant algorithms [7] provide essential answers to ensuring security systems are ahead of the curve, but each has practical drawbacks. For these techniques to become the norm, they will need optimisation for speed and size and simplifying how keys are handled. Additionally, they may be scaled successfully across many contexts or devices. A balanced approach may occasionally be provided by mixing quantum and classical cryptography techniques, and further development will help make these algorithms more beneficial for the many demands of our increasingly digitised society. In this analysis, we explore the technical components of these methods in further depth.

3.1 | Blockchain vulnerabilities to quantum attacks

How quantum algorithms (Shor and Grover) threaten the integrity of current blockchain systems.

1) How Shor's algorithm threatens blockchain:

- It can efficiently break RSA encryption due to its ability for factorising large numbers.

Breaking ECC–Shor's algorithm can solve the elliptic curve discrete logarithm problem.

2) How Grover's algorithm threatens blockchain:

- Symmetric encryption and hash functions
- Symmetric security

3.2 | Analysis of why public-key cryptography in blockchain (like ECDSA) is vulnerable to quantum computers

ECDSA (elliptic curve discrete logarithm problem) is an algorithm that relies on the elliptic curve discrete logarithm problem.

- This problem cannot be computationally solved by classica algorithms, and algorithms like the Shor's algorithm can easily break this scheme.
- Private key is recovered using the public key, and then forging the signatures and stealing funds can be done.

TABLE 3 Real-world blockchain trade-offs.

Scheme	Security	Key size	Encryption/decryption speed	Signature size
RSA	Secure against classical attacks	Large (2047–3072 bits)	Fast encryption, slow decryption	Large
ECC	Against classical attacks	Small (256–384 bits)	Fast	Small
Dilithium	Secure against both	Medium (1024–2048 bytes)	Fast encryption, medium decryption	Medium
Kyber	Secure against both	Medium (1024–2048 bytes)	Fast encryption, decryption	Medium

- A quantum computer with sufficient number of qubits can break this scheme in hours or even minutes.

3.3 | Integrating lattice-based cryptography into blockchain

Lattice-based cryptography can replace classical cryptographic algorithms with quantum-resistant cryptographic schemes.

- Lattice-based digital signatures in blockchain, such as Dilithium, provide a quantum-resistant alternative to ECDSA.
- LATTICE-based key exchange—Kyber
- Challenges faced—larger key and signature sizes, backward compatibility, and performance overhead.
- Transition strategies for blockchain—hybrid cryptographic systems, soft fork or hard fork.

3.3.1 | Step-by-step process of incorporating lattice-based cryptographic techniques into blockchain systems

a) Select a lattice-based cryptographic algorithm—to consider security, efficiency and NIST standardisation.
b) Redesign key generation and transaction signing mechanism—lattice-based key generation and digital signatures.
c) Update verification mechanism for lattice-based signatures.
d) Integrate lattice-based key exchange—secure node communication and smart contract interaction.
e) Optimise for performance and scalability.

3.3.2 | Quantum-resistant key exchange: Using Kyber for establishing secure channels in blockchain

Quantum computers pose a significant threat to cryptographic security of blockchain systems, particularly in key exchange protocols. Kyber is a lattice-based key encapsulation mechanism based on the LWE problem. The Kyber-based key exchange process includes steps such as key generation, encapsulation, and decapsulation. Main advantages of this are secure node to node communication, off chain communication and layer 2 protocols.

3.3.3 | Quantum-resistant digital signatures: Using Dilithium to replace ECDSA in smart contracts

Quantum computers can efficiently break ECDSA, which compromises security of blockchain systems. Dilithium is based on LWE and SIS problems and offers key advantages such as quantum resistance, efficiency and NIST standardisation. Dilithium uses a lattice-based approach for generating public and private keys. Some important steps are key generation, transaction signing, and signature verification.

3.4 | Security and scalability

3.4.1 | Analysis of the security level provided by lattice-based cryptography in blockchain networks

- Quantum resistance—lattice problem hardness.
- Resistance to classical attacks—lattice reduction algorithms and concrete security levels.
- Protection against quantum attacks.
- Long-term data integrity.
- Secure smart contacts.
- Implementation considerations for blockchain—key and signature sizes and hybrid systems.

3.4.2 | Discussion on key size and storage issues related to lattice-based schemes in blockchain implementations

- Key size—larger than ECC or RSA.
- Signature size—cause increased transaction size and larger block sizes.
- Mitigation strategy—compression techniques, batch verification, and storage offloading.

3.4.3 | Examples of blockchain projects already integrating or researching quantum-resistant cryptographic techniques

- Quantum-resistant ledger
- IOTA
- Algorand
- Ethereum
- Hyperledger

3.5 | Strengths and weaknesses of key quantum-resistant algorithms

1. **Lattice-based cryptography**

Merits: This encryption method possesses a significant advantage due to its utilisation of intricate mathematical structures known as lattices. Lattice issues are exceedingly challenging for classical computers, suggesting that quantum computers may perform far better. Consequently, the lattice-based cryptography schemes are flexible and appropriate for encryption, signatures, as well as secure key exchanges using quantum-resistant algorithms.

Demerits: The computationally intensive nature of lattice-based cryptography approaches may result in efficiency and scalability problems. The real-time processing is the bottleneck in different IoT-based lightweight devices because of huge computational demand on them.

2. Hash-based cryptography

Merits: Hash-based [8] solutions, such as Merkle trees are quite practical to implement. They are currently used for data authentication and digital signatures, with performance characteristics intermediate between hash-based approaches and lattice-based ones.

Demerits: Hash-based cryptography generally requires very frequent key changes, and normally it would be only for single-use (not really inefficient for many repetitions of usage). As a result, it is not suitable for applications that require frequent data exchange at high speed because then the memory block has larger hash structures and tends to become unwieldy.

3. Multivariate polynomial cryptography

Merits: These are difficult polynomial equations (in fact, they are a nice example of an NP-complete problem) and quantum computers will not solve them quickly. Multivariate polynomial cryptography [9] is especially useful for secure key exchange and digital signatures, since they provide an exceedingly high level of post-quantum attack security.

Demerits: Key handling in multivariate polynomial cryptography can be cumbersome and this is particularly relevant for mobile or IoT applications, which frequently have only a modest amount of computational horsepower. That can be difficult to implement particularly for cases that require lightweight processes.

4. Code-based cryptography

Merits: Code-based cryptography [10] is one of the most battle-tested quantum-resistant techniques; it has a good track record. It's security capability is top-notch, so it can be used for secure email and key exchanges. Due to this nature, the major cloud providers and other commercial solutions use this cryptography, especially in the software industry.

Demerits: The negative point with code cryptography is that it needs large key sizes which can be space hungry and potentially increase the transmission overhead. When there is not a lot of bandwidth around, or on low-powered devices, this results in a problem.

5. Isogeny-based cryptography

Merits: It has small key sizes, which makes it efficient and well-suited for key exchange applications like the super-singular isogeny key exchange (SIKE) [7] protocol. This will make easier for the delivery and storage of key exchanges—one reason why it is so popular in low bandwidth and expensive data contexts.

Demerits: However, this method is primarily applicable to quantum-resistant algorithms than general-purpose key exchange mechanisms. And it can also be slow at high speeds; therefore, some applications which require real-time performance might not get a benefit out of it.

Table 4 lists a few notable quantum-resistant cryptography algorithms, their complexity, computational load, feasibility for low-power devices, applications, and key metric formulas.

4 | QUANTUM BLOCKCHAIN-BASED SECURITY MECHANISMS

The emergence of quantum computing presents a paradigm shift that could disrupt current cryptographic methods used in blockchains. Quantum computers, leveraging principles like superposition and entanglement, threaten classical cryptographic algorithms such as RSA and ECC (elliptic curve cryptography). To address this, the concept of quantum blockchain has emerged, combining quantum cryptographic techniques to enhance the security and resilience of distributed ledger systems. Figure 7 summarises the elements of a quantum blockchain and the security concerns for the future.

The core security mechanisms in quantum blockchain involve

1. **Post-Quantum Digital Signatures**: Replacing classical signatures with post-quantum options such as those based on LWE or multivariate quadratic equations ensures that

TABLE 4 Comparison of quantum-resistant cryptography algorithms.

Algorithm	Complexity (time)	Computational load	Suitability for low-power devices	Typical applications	Key metric/Formula
Lattice-based cryptography	Exponential (O (2^n))	High	Moderate to low	Blockchain, digital signatures	Hardness of **Learning with errors (LWE)**: LWE (n, q)
Hash-based cryptography	Polynomial (O (n^2))	Low to moderate	High	Digital signatures, authentication	**Merkle Tree** Height Formula: H = $\log_2(N)$
Multivariate polynomial cryptography	NP-hard	High	Low	Public key encryption, digital signatures	**System of polynomials**: Solving P $(x_1, x_2, \ldots, x_n)$ = b
Code-based cryptography	Polynomial (O (n^3))	High	Moderate to low	Key exchange, secure communications	Error correcting code for syndrome Decoding: syndrome = H*m

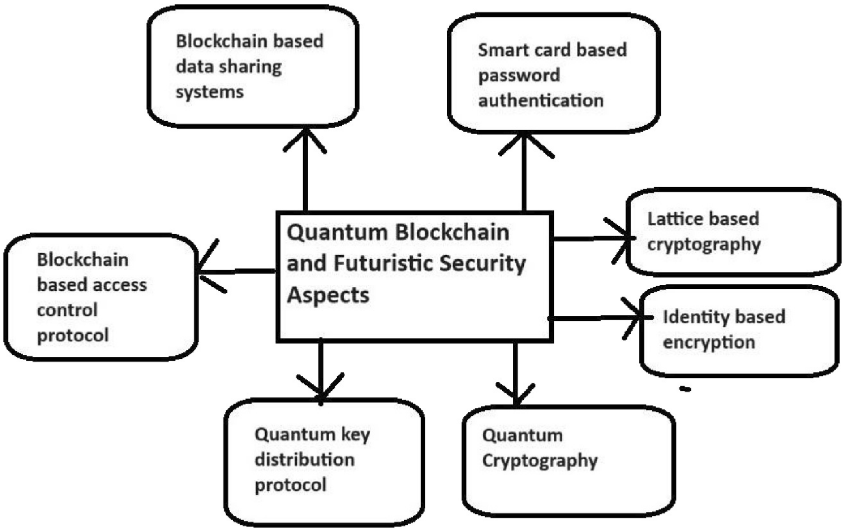

Blockchain based data sharing systems
Smart card based password authentication
Quantum Blockchain and Futuristic Security Aspects
Lattice based cryptography
Identity based encryption
Blockchain based access control protocol
Quantum key distribution protocol
Quantum Cryptography

FIGURE 7 Quantum blockchain and futuristic security aspects.

even quantum computers cannot forge digital signatures, maintaining blockchain integrity.

2. **Quantum-Safe Key Exchange Protocols**: Traditional blockchains use public key infrastructure (PKI) for key exchange, which is vulnerable to quantum decryption. Replacing these with PQC-based methods, such as hash-based or lattice-based schemes, ensures quantum safety during transactions.

Quantum-Enhanced Consensus Mechanisms: Although still theoretical, models leveraging quantum entanglement could create new consensus protocols that promise faster verification and reduced energy consumption compared to classical methods.

4.1 | Challenges in quantum blockchain implementation

Despite these advancements, implementing quantum-resistant blockchain comes with significant challenges:

- **Technological Readiness**: Quantum technology is still in its nascent stages, limiting real-world deployment. Building quantum-safe blockchains requires significant investment in infrastructure capable of handling quantum-based operations.
- **Complexity and Scalability**: Integrating quantum-safe cryptographic algorithms can be computationally intensive, potentially impacting the performance and scalability of blockchain networks.
- **Compatibility Issues**: Transitioning current blockchain systems to quantum-resistant models requires careful consideration to maintain backward compatibility with existing systems and protocols.

A quantum blockchain is a geographically dispersed, encrypted, and distributed database built on the principles of quantum information systems and quantum computation. It boasts decentralisation, transparency, and tamper resistance, making it valuable across diverse applications such as information security, digital currencies, and smart contracts. Blockchain security integrates cybersecurity principles, tools, and best practices to prevent unauthorised access and malicious attacks on blockchain networks. This research delves into security frameworks in quantum blockchain, focusing on cybersecurity, blockchain security in healthcare, cryptography, and defence mechanisms against quantum attacks. Various quantum blockchain-based security schemes available in the literature are summarised in Table 5.

5 | QUANTUM BLOCKCHAIN-BASED AUTHENTICATION PROTOCOLS

An authentication protocol is a specific computer or cryptographic protocol crafted to facilitate the secure transfer of authentication data between two entities. Blockchain authentication ensures a secure verification process within the blockchain network, enhancing transaction security and transparency. The objective of Internets of Vehicle (IoV) systems is to establish connections between several vehicles, facilitating the sharing of vital information under an IoT-enabled network.

A novel certificate-less data authentication protocol has been developed to enhance security in open wireless communication. This protocol also mitigates quantum attacks by leveraging lattice cryptography. The algorithm guarantees both fundamental unforgeability and superior performance compared to current methods in relations of data processing, energy consumption, and overheads associated with cryptographic key storing.

Many automobiles are interconnected by the Internet of Automobiles (IoAT) technology, facilitating the interchange of substantial data over an Internet of Things (IoT) network. Historically, data authentication in the Internet of Vehicles

TABLE 5 Quantum blockchain-based security schemes.

Name of paper	Authors	Year	Application	Key findings
Quantum blockchain with asymmetric quantum encryption and stake voting consensus [11]	Wusheng Wang, Yang Yu, Lingjie Du	2022	DPoSB for transaction security using quantum signatures	Combines DPoS with borda count consensus and QRNG for enhanced security in quantum-resistant blockchains.
Ensuring optical network security through quantum-secured blockchain [12]	Purva Sharma et al.	2023	Optical network security with quantum-secured blockchains	Review of QKD-based quantum-safe blockchain technology for network security.
Lattice-based signature scheme for post-quantum blockchain [13]	Chao-Yang Li et al.	2019	Securing blockchain with classical stations	Lattice-based signatures using bonsai trees and randbasis for lightweight wallets.
Blockchain cybersecurity for IoT smart cities [14]	Ahmed A. Abd El Latif et al.	2021	Securing IoT data sharing	Quantum-inspired quantum walks for efficient IoT data exchange.
Resistance to quantum computing in blockchain networks [15]	Marcos Allende et al.	2023	Post-quantum blockchain framework	Proposed end-to-end framework with open-source Ethereum implementation.
Blockchain model for healthcare based on quantum trust [16]	Shitharth Selvarajan, Haralambos Mouratidis	2023	Secure healthcare data transfer	Consultative transaction key management using random () and multiply () functions.
Hybrid scheme for healthcare 5.0 with blockchain and quantum blind signatures [17]	Makwana Bhavin et al.	2021	Healthcare blockchain architecture	Blockchain-based architecture with quantum blind signatures for secure data access.
PQFabric: Quantum and classical attack-resistant blockchain [18]	Amelia Holcomb et al.	2021	Permissioned blockchain security	Hybrid signatures in PQFabric for cryptographic agility and attack resistance.
Blockchain with quantum-resistant digital signatures [19]	Peijun Zhang et al.	2021	Optimising blockchain performance	Hashing public keys and signatures for efficient transaction size and bitcoin exchange evaluation.

(IoV) has been characterised by complex certificate administration based on the Diffie–Hellman (DH) hypothesis. Nevertheless, DH-type issues are susceptible to quantum cryptanalysis, which can answer them in a polynomial time. To safeguard open wireless communication in the Internet of Vehicles (IoV) against quantum assaults, D.S. Gupta et al. [20] have suggested a new no-certificate data verification protocol that utilises lattice cryptography. Furthermore, it integrates a resilient blockchain engine to guarantee the reliability of automobiles using batch data validation. An exhaustive investigation of the proposed protocol has shown its robustness against existential forgery in chosen message assaults. Furthermore, it provides integral security functionalities such as unthinkability, restricted traceability, anti-replay protection, and data truthfulness. Comparative presentation assessments demonstrate that this novel protocol surpasses current energy ingesting, data processing speed, communiqué efficiency, and cryptographic significant storage needs.

The increasing need to advance road safety and streamline transportation flow has emphasised the significance of vehicular ad-hoc networks (VANETs). To tackle the problem of unidentified verification for safety messages while ensuring traceability to authority, R. Lu et al. [21] propose a highly effective approach for maintaining conditional privacy in VANETs. The present protocol facilitates the real-time generation of short-term anonymous keys amid on-board units (OBUs) and roadside units (RSUs). This methodology facilitates quick, anonymous verification and privacy monitoring while reducing the storage needs for temporary anonymous keys. Thorough investigation and analysis have illustrated the substantial advantages provided by this approach.

A secret key that both parties share is used in symmetric key cryptography to ensure the security of network communications. The sender and recipient are the only parties that know this key, and they use it to encrypt and decrypt messages. Key exchange protocols are specialised protocols that enable the sender and recipient to establish a shared secret key. Traditionally, the security of these protocols relies on the solution of Diffie–Hellman (DH) problems, which quantum computers can attack. Hence, it is necessary to develop alternate key exchange systems immune to quantum computers. In their study, Gupta et al. [22] provide two innovative lattice-based authenticated key exchange (AKE) protocols within the framework of the Canetti–Krawczyk proof model. The two protocols use distinct methodologies: one uses a signature-based authenticator, while the other utilises an encryption-based authenticator. The safety of these suggested rules is contingent on the challenge of finding feasible results for small integers within lattices. Advanced knowledge Iinference systems (AKEs) are recognised for their superior computational speed and robustness against contemporary, intricate computer technology.

Vehicular ad-hoc networks are vital for managing contemporary transport communication in which mobile automobiles function as nodes to establish a mobile system. Vehicular ad-hoc networks (VANETs) enable the transmission and monitoring of wireless traffic information between participating vehicles or nodes. Before implementation, VANETs integrate a privacy mechanism to guarantee safe network communication. The paper by S. Mukherjee et al. [23] presents many conditional privacy-preserving authentication methods that guarantee mutual protection and authentication.

The systems mentioned are the initial examples of lattice-based restricted privacy-preserving validation. Security research shows that the suggested protocol simultaneously maintains message dependability, verification, and confidentiality protection using a random oracle model.

Given the growing digitisation of businesses, two dynamic technologies, cloud computing and the Internet of Things (IoT), substantially impact contemporary organisations. Many enterprises delegate their crowd-sourced industrial Internet of Things (IIoT) data to cloud-based environments. Therefore, it is imperative to provide data authentication as a crucial security prerequisite in IIoT networks. This requirement for data authenticity in IIoT systems is met by implementing a certificateless signature (CLS) method. The primary reason CLS has attracted considerable research interest is its capacity to address the fundamental problem of key escrow in contemporary identity-based signature methods. Typically, these CLS systems employ a map-to-point (MTP) hash function and the random oracle model (ROM).

Nevertheless, the practical execution complexities and probabilistic characteristics of the MTP function and ROM give rise to practical implementation issues. In their study, Karati et al. [24] propose a novel pairing-based CLS technique that prevents the MTP function and ROM requirement. By exploiting the robustness of comprehensive bilinear strong Diffie–Hellman norms, this novel approach guarantees protection against type-I and type-II challengers.

A reputation management method is crucial for ensuring effective communication security in-vehicle networks. In recent years, conventional solutions have faced challenges in matching the improved network performance of 5G networks. To fill this void, a novel integrated detection and elimination system (IDES) is presented by S. Su et al. [25]. The IDES system incorporates an integrated reputation mechanism to identify and isolate rogue nodes in the vehicular system. The system architecture is strategically developed to incorporate our reputation management system, considering possible danger situations in large detail. The effectiveness of IDES is thoroughly assessed by employing a custom-built event-based emulator to replicate malicious assaults. Findings illustrate the scheme's efficacy in countering three different attack mechanisms, highlighting its greater responsiveness compared to existing decentralised trust management systems.

The Internet of Vehicles (IoV) is an advanced ad-hoc network designed to improve highway traffic efficiency. When operating in an open wireless environment, the Internet of Vehicles (IoV) encounters difficulties because of its changing network topology, which adds complexity to the dispensation and figuring of mobile services. Vehicles in this network communicate real-time data like their location, orientation, and velocity to alleviate traffic congestion and avoid collisions. Nevertheless, the lack of sufficient security mechanisms presents substantial hazards, considering the many malevolent attackers. In their study, Wang et al. [26] present a highly efficient decentralised authentication system for the Internet of Vehicles, which utilises the consensus algorithm of blockchain technology. The system aims to improve security by mitigating self-centred behaviour and defending against malicious attacks. The viability of the hypothesised mechanism is confirmed through simulations performed within the Veins framework.

The Internet of Vehicles (IoV) is an innovative development in smart transportation structures. Commonly, intelligent vehicles are outfitted through onboard units, sensors, GPS, and other advanced technology. The Internet of Vehicles (IoV) facilitates communication between these vehicles through high-speed Internet connections. The inherent mobility of automobiles presents difficulties in sustaining strong network connections. Implementing cooperative communication offers a viable approach to optimise communication efficiency, mitigate delay, and decrease packet loss and drop rates (PDR). To overcome these difficulties, Akhter et al. [27] suggest implementing a blockchain-based authentication structure to guarantee the security and privacy of the Internet of Vehicles. Authentication information is stored and managed in a decentralised environment using blockchain technology. The protocol, created on the Ethereum platform, employs a digital mark mechanism to maintain the privacy, integrity, and non-repudiation of electronic interactions.

Clinical cyber-physical systems (MCPS) provide supple communications between patients and medical systems, serving as the foundation of intelligent healthcare applications. P. Gawali et al. [28]examine a device identity identification system essential for guaranteeing the necessary security and dependability of MCPS. To comply with strict security standards, the study suggests a robust authentication technique to protect confidential healthcare information. More precisely, a modified adaptation of the "elliptic curve Diffie–Hellman" encryption method encrypts medical data obtained from patients before it secures storage in the cloud. This method guarantees regulated access to stored data for the specific purpose of medical data analysis. Moreover, a quantum key distribution architecture improves the management of encryption keys to provide additional security. Furthermore, the research investigates the incorporation of blockchain technology to enable a reciprocal authentication of users in MCPS infrastructures. This blockchain-based approach enhances the authentication framework, improving trust and security in medical cyber-physical systems.

The procedures of key distribution protocols include the development, exchange, and storage of information, specifically shared keys. In this study, Gheorghies et al. [29] compare three fundamental protocol types: classical, quantum key distribution, and blockchain-based protocols. This paper provides instances from each category, elucidating their distinct features, difficulties, suggested remedies, and the overall influence of these protocols. Key dissemination protocols play a vital part in contemporary cryptography by enabling the implementation of more efficient asymmetric cryptography methods.

Gao et al. [30] present a novel approach to enhance the security of ring learning with errors (RLWE)-based key exchange protocols against signal leakage attacks. By introducing a randomised, ephemeral public error term, the proposed protocol mitigates the risk of key exposure in scenarios where

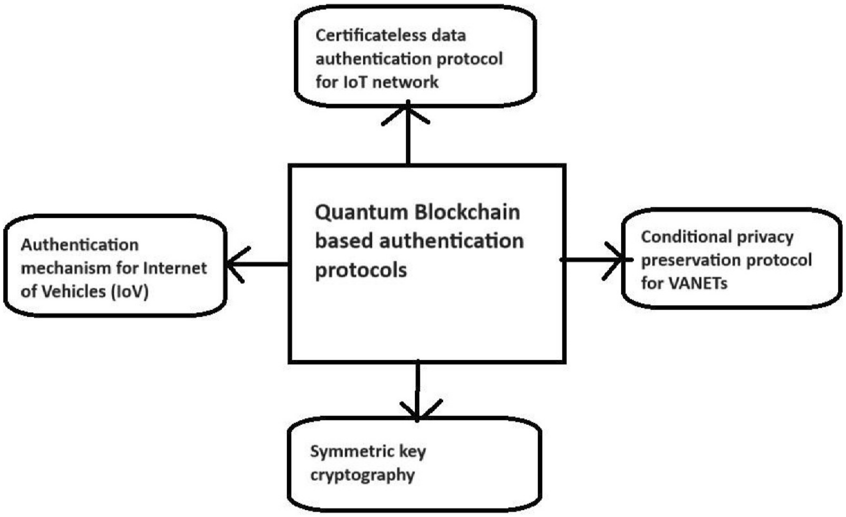

Certificateless data authentication protocol for IoT network
Authentication mechanism for Internet of Vehicles (IoV)
Quantum Blockchain based authentication protocols
Conditional privacy preservation protocol for VANETs
Symmetric key cryptography

FIGURE 8 Quantum blockchain-based authentication protocols.

key reuse is necessary, such as in transport layer security (TLS). Benchmark tests validate that this modified RLWE-based protocol not only withstands attacks but also maintains high efficiency, potentially outperforming vulnerable protocols. The paper proposes a solution that aims to defend against signal leakage attacks without incurring significant performance penalties. Unlike previous approaches requiring costly transformations or complete avoidance of key reuse, this protocol maintains efficiency by introducing an ephemeral error term during each key exchange. By introducing this random term, the modified protocol disrupts the attacker's ability to exploit signal leakage, as the signal values now appear uniformly random. This adjustment aligns with TLS's performance requirements, providing a lightweight, practically deployable solution.

The significance of Quantum blockchain-based authentication procedures in modern cryptographic frameworks is depicted in Figure 8.

6 | AI FOR QUANTUM BLOCKCHAIN

The collaboration between quantum computing and artificial intelligence grants substantial promise, leveraging the distinct capabilities inherent in quantum computers. Quantum AI [31] merges quantum computing with artificial intelligence, harnessing quantum states that exploit superposition and entanglement for parallel processing. Advanced quantum algorithms significantly enhance efficiency in data analysis and pattern recognition tasks, enabling optimisation, cryptography, and machine learning applications. Using quantum mechanical sensations like chance polarisation of photons or quantum tunnelling of electrons to yield arbitrary numbers, quantum communication emerges as the most secure technique for data conveys. The combination of quantum-supported artificial intelligence (AI) and machine learning (ML) algorithms increases the quality of random number generation processes by facilitating the analysis of data patterns and the detection of biases.

Obtaining detailed and current information on the location and behaviour of wildlife would significantly enhance our ability to study and conserve ecosystems. Motion sensor cameras play a crucial role in gathering vast amounts of data on wild animals. However, manually analysing each image is impractical. In M.S. Norouzzadeh et al. [32], cutting-edge artificial intelligence, specifically deep neural networks, automates the extraction of invaluable information from these datasets. Advanced deep learning techniques provide precise and reliable automatic animal identification, achieving a 99.3% accuracy rate on the 3.2 million photos in the Snapshot Serengeti dataset. By streamlining and accelerating research activities, this automated and cost-effective data-collecting method can potentially transform ecology, wildlife biology, zoology, and conservation biology.

Undertaking rigorous study and extracting valuable knowledge from extensive datasets presents considerable obstacles. The incorporation of quantum computing is driving continuous advancements in big data analytics. T.A. Shaikh et al. [33] thoroughly examine the current body of scholarly work on the usage of quantum computing methods in machine learning for big data analytics. This paper classifies quantum machine learning into several subfields and examines the use of quantum walks in the construction of quantum artificial neural networks. These networks significantly improve the promptness of quantum machine learning algorithms. A comparative analysis is conducted between quantum supervised and unsupervised machine learning and its classical equivalents, emphasising the benefits of quantum methodologies. Furthermore, the article analyses the constraints inherent in existing machine learning methods and tools while highlighting the possibilities and difficulties linked to quantum computing technology.

A conceptualisation of the design for a universal Internet of Things (IoT) that integrates quantum cloud computing with blockchain is presented. The quantum computing chip in W. Dai [34] is conceived and modelled as a multi-input multi-output (MIMO) quantum channel. The value of its channel ability is calculated by a newly developed mutual information method. The channel modelling utilises a profound convolutional neural network with widespread stochastic merging to capture the supply allocation dynamics amid various eigenmodes or consumers. The scheduling strategy integrates a saddle point method for zero-sum game problems with a Pareto optimum Nash equilibrium fact for non-zero-sum game submissions.

Artificial intelligence and blockchain technology fields are seeing fast growth, each characterised by different degrees of intricacy and multifaceted commercial prospects. Together, they construct more intelligent, secure, efficient, and resilient systems. Nevertheless, these technological breakthroughs are also becoming more vulnerable to quantum attacks. The paper by B. Yuan et al. [35] grants a lattice-based blockchain framework designed for artificial intelligence and created to be immune to quantum attacks. This architecture optimally utilises lattice-based collective signatures to control the distribution of signatures within chunk sizes efficiently. Validation of the suggested technique for security within the random oracle model and demonstration of higher efficiency compared to current literature. This work exhaustively scrutinises post-quantum blockchain transactions, including a detailed analysis of their implementation and security factors.

By enabling automated patient monitoring, easing data collecting from sensors, and ensuring secure data storage, blockchain technology and its accompanying procedures are poised to change future healthcare systems. This feature reduces the necessity for frequent interventions by effectively and safely storing large amounts of data. Leveraging the capabilities of quantum computing via quantum blockchain technology holds great potential for substantial progress. Novel functionalities including quantum computing-based thermal imaging and fast patient localisation and observing are expected to provide significant advantages. The conjunction of quantum computing and blockchain technology expedites the processing of medical records while guaranteeing confidentiality. The potential advantages and implications of blockchain and quantum technologies in healthcare systems are investigated by K. Kaushik et al. [36]. Their study investigates the relative benefits of quantum technologies and blockchain-based solutions in conjunction with advanced information and communication technologies such as artificial intelligence, machine learning, and drones.

Climate change-related global challenges, such as heatwaves in California and Canada and floods in Germany and India, are progressively threatening the habitability of Earth. Significant advancements have been observed in numerical weather and climate modelling, aiming to minimise the loss of life and property through spatially and temporally precise forecasting. Advanced artificial intelligence (AI) techniques are essential in improving these forecasts. In M. Singh et al. [37], the focus is on exploring quantum artificial intelligence (QAI) algorithms specifically designed for quantum computers to advance climate change research. These developments are aimed at leveraging QAI to innovate and refine climate prediction and mitigation approaches.

A quantum blockchain is an autonomous, encrypted, and distributed database that implements concepts derived from quantum computing and quantum information theory. Information stored in a quantum blockchain is impervious to security breaches by evil entities. In their study, Li et al. [38] present a complete analysis of the cutting-edge progress in quantum blockchain technology, emphasising its superiority compared to traditional blockchain systems. The authors thoroughly examine the structure and outline of quantum blockchain, investigating the potential of quantum technology to augment some elements of conventional blockchain protocols.

The integration of AI and blockchain signifies a revolutionary technological transformation. Datasets might incur significant expenses, liable on the meticulous variety of individual components and the guarantee of data uniformity. Blockchain technology, known for its exceptionally secure storage capabilities, is a breakthrough in preserving data integrity. Implementing artificial intelligence (AI) and blockchain technology can completely transform several sectors, such as IoT (Internet of Things), self-authentication, financial fairs, and keen cities. A study by K. Sgantzos et al. [39] examines the advantages and disadvantages of this groundbreaking expertise.

Integrating quantum computing and artificial intelligence signifies the advent of a novel epoch for Industry 4.0. The study by How et al. [40] explores the complexities of quantum AI, examining its significant influence on Industry 4.0 and providing crucial transformation board and novelty approaches for smooth combination. Incorporating theoretic perspectives and empirical examples, the study examines the present state of quantum AI. The critical focus is on change management strategies, promoting ongoing education, cooperative environments, and proactive methodologies. This study emphasises the need to actively embrace quantum AI advancements and investigate its wide range of applications. This promotes the use of planned forethought, interdisciplinary association, and strong risk administration to prepare participants with the necessary information and methods to effectively direct the intricate aspects of quantum AI in the context of Industry 4.0.

A dispersed record, sometimes identified as a blockchain, is a distributed database in which every logged transaction is digitally signed using a unique private key. All modifications made to the ledger can be attributed to particular public-private key pairs, and each atomic operation is permanently recorded after the database mathematically verifies its integrity and distributed consistency. K. Kalafatic [41] demonstrates how the mathematical principles of blockchain can improve learning in artificial intelligence and strengthen security protocols.

The study by Ramos and Ellul [42] investigates using blockchain technology to address certain cybersecurity threats linked to artificial intelligence (AI) systems. Our research focuses on AI legislation's data supremacy, record-keeping, transparency, and access control criteria. This paper illustrates the efficacy of blockchain skill in justifying specific attack vectors related with artificial intelligence (AI), such as data harming in trained AI prototypes and datasets. This paper examines the application of parameters to limit access to crucial AI systems enforced using private keys. Furthermore, it explores the possible of blockchain technology to offer autonomous audits and validate AI system performance. Furthermore, it emphasises the capacity of blockchain to improve the robustness of high-risk AI systems against cyber threats, thus promoting secure implementations of AI technologies. The study generally seeks to connect legal and technical research, offering critical insights to policymakers in making well-informed judgements about AI cyber risk management.

Various communities and research organisations are actively pursuing the realisation of quantum computing applications. Concurrently, artificial intelligence continues to evolve as a potent and stable tool. The objective of B. Rawat et al. [43] is to evaluate the influence of quantum computing research on artificial intelligence applications. The work utilises computational methods to analyse and measure this influence systematically. This paper examines the possible influence of quantum computing research on developing artificial intelligence applications. Furthermore, the authors investigate the possible consequences and probable advantages that quantum computing could provide in artificial intelligence.

C. Jones et al. [44] aim to critically review the complex issue of financial exclusion and evaluate whether AI and other innovative technologies can offer solutions. The chapter provides recommendations to government officials and policymakers on their pivotal role in crafting effective, human-centred, understandable, and useable regulations to support AI in banking. The chapter argues that although a complete eradication of financial exclusion may not be possible and there is no one answer, advancement can be made by gradually tackling its underlying causes. Artificial intelligence (AI) offers a promising solution, provided it is duly controlled and included in financial systems.

The emergence of quantum skills based on the important values of quantum physics is transforming smart city ambitions. In their study, A.B. Bonab et al. [45] investigate the managerial consequences of urban quantum technologies in shaping future smart cities. The research examines the possible of quantum technologies to progress smart city elucidations, which include the cloud computing, Internet of Things, big data, smart transportation, blockchain processes and artificial intelligence. The study constitutes a semi-ordered examination of 80 papers about quantum computing in social science. This paper delineates two fundamental concepts, such as quantum computation and quantum communication. Furthermore, the research utilises the automated text analysis of 567 abstracts to construct a thorough classification of traditional smart city systems. Moreover, the study investigates possible synergies between traditional smart city results and urban quantum technologies by the analysis of the connections among the 80 quantum technology papers.

7 | QUANTUM BLOCKCHAIN AND QUANTUM WALKS FOR CRYPTOGRAPHY AND IMAGE PROCESSING

- **Quantum Blockchain**

At present, quantum blockchain technology is primarily researched within the field of quantum cryptography. A blockchain serves as a ledger containing transactional history data. Its current design makes tampering with a blockchain challenging, as it does not require centralised control to maintain ongoing accuracy. Nevertheless, the advent of quantum computing postures an important challenge for the characteristics of blockchain technology [46].

Ledger: The ledger comprises a sequence of blocks, each containing the value of hash of the header of the previous block in the chain, a date, a block ID, and a list of transactions. Furthermore, it secures the ownership and precise whereabouts of all existing currencies.

Proof of work: The users are required to publish transactions regularly. A block will be deemed acceptable only if it comprises legitimate evidence of effort.

Proof of Stake: The feasible mining power is directly proportional to the quantity of coins own by the miner.

Proof of Burn: Works on the norm of permitting miners to "burn" virtual currency proofs. POB is also called a proof of work system without energy waste.

Smart contracts: Blockchain 2.0 uses autonomous agents called smart contracts. Here, ledgers are accounts, not coins. The record contains the account's 20-byte key address (a public key value), ID, remaining amount, agreement code, and storage. Externally owned accounts (EOA) and contract accounts (CA) are their types. Private keys organise the EOA and contract codes organise the CA.

Quantum Coins are the fundamental data arrangements to express a crypto currency blockchain. There are various types of coins, such as public-key quantum money, binding commitments, collapsing hash functions, collision-free quantum memory, and quantum lightning. Due to the emergence of quantum computers, current cryptographic systems are anticipated to encounter significant challenges in the foreseeable future. Currently, these systems depend on complex mathematical problems that quantum computers can effectively solve within a finite polynomial timeframe. Two primary methodologies have been suggested to tackle this problem: the first is creating cryptographic designs impervious to quantum attacks, like lattice-based encryption and hash-based cryptography. The second strategy investigates the utilisation of principles derived from quantum blockchain. Literature includes discussions on quantum-resistant blockchains that are intended to replace existing permissionless and quantum-secured blockchains aimed at replacing permissioned ones.

7.1 | Quantum walk operations

Quantum walks represent a quantum protocol grounded in advanced mathematical principles. They serve as search algorithms within graphs, initially introduced by Yakir Aharonov et al. [47]. Problems in graph theory that leverage quantum walks can be resolved in quadratic or polynomial time, whereas classical algorithms typically require exponential time for similar tasks. Quantum walks have been successfully applied to problems such as locating triangles within graphs [48].

Kendon and Sanders investigated a correlation between complementarity notions and quantum walks [49]. Table 6 shows a comparative analysis of quantum walks and classical walks.

- **Implementing Quantum walk using IBM's Qiskit**

Figure 9 depicts the quantum circuit for implementing a quantum walk [50] using IBM Quantum Experience Qiskit. The circuit uses a Hadamard gate, a CNOT gate, and a CCNOT gate for implementation.

The diagram in Figure 10a illustrates the output of the quantum circuit in a state vector form, whereas Figure 10b presents the histogram output. It indicates that when running the code on ibmq_qasm_simulator, there is a 50% probability for the walker to transition from the state |000> to either |001> or |011>. The same circuit was executed on a real quantum device, specifically IBM Quantum Experience's ibmq_bogota [51], and the results are illustrated in Figure 10c. On the real device, measurements included states such as |000>, |100>, and |101>, which are attributed to gate and qubit errors, namely noise inherent in real-world devices.

7.2 | Contributions based on quantum blockchain and quantum walks

There exist two distinct categories of quantum walk-based systems known as discrete-time walks, characterised by discrete step evolutions, and continuous-time walks, characterised by evolution along a continuous Hamiltonian. Quark phase kickback is a fundamental interference method employed in quantum machine learning, oracle-based search algorithms and quantum walks. Table 4 provides a complete summary of the many references in the literature which specifically examine the applications of quantum blockchain and quantum walks in cryptography and image processing. A statistical comparison of blockchain technology in cryptography and image processing applications is presented in Table 7.

Key terms related to quantum cryptography are quantum memory, quantum signatures, quantum security etc., are presented in Figure 11.

Key terms related to quantum image processing are entangled image, quantum database, quantum images etc., are presented in Figure 12.

TABLE 6 Quantum walk versus classical walk.

	Quantum walk	Classical walk
Paths	Exploits the quantum superposition principle to simultaneously traverse all possible routes, enabling concurrent movement along numerous paths.	A walker will have the possibility of moving towards one path only.
Matrix	Unitary matrix	Stochastic matrix
Evolution	Reversible	Irreversible
Spreading behaviour	Faster	Slow
Measurement-position of walker	Amplitude measurement	Probability
Behaviour	Non-ergodic behaviour	Ergodic or non-ergodic
Constructive and destructive interference	Applicable	Not applicable
Randomness	Depends on the measurement operation at the end	Move from one position to any of the nearest positions
Complexity	Solves problems in quadratic or polynomial time	Solves problems in exponential time

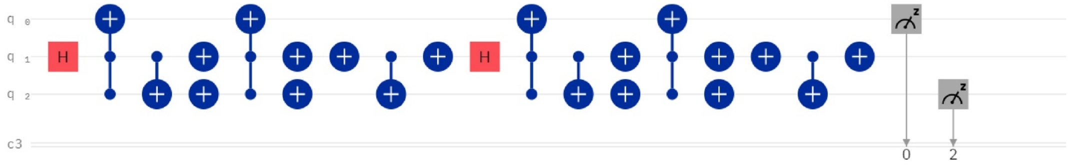
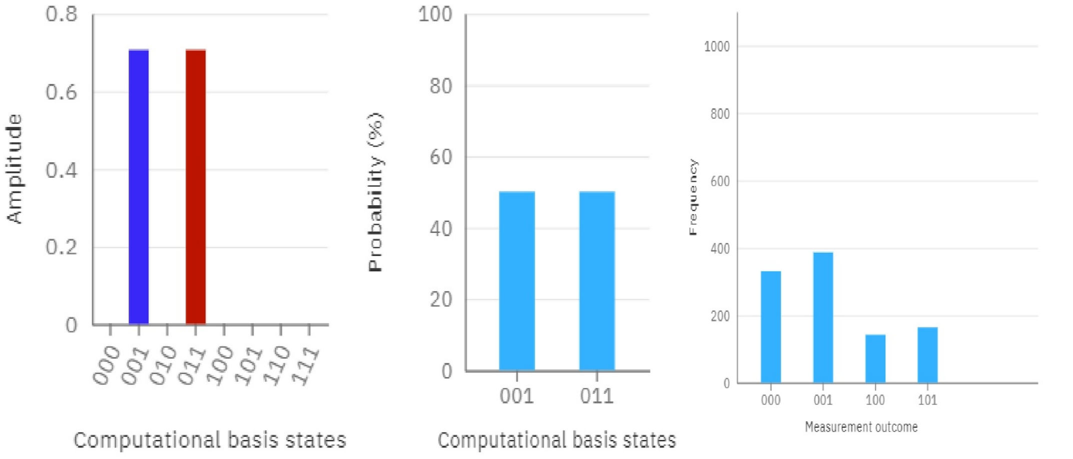


FIGURE 9 Quantum walk circuit realised using IBM Qiskit.



a) State vector Representation b) Histogram c)Real Quantum Computer

FIGURE 10 Output of the three-qubit quantum walk circuit.

TABLE 7 Comparison table.

Author	Year	A	B	C	D	E	Application	Key Finding
Baniata, Anaqreh, Kertesz [52]	2021	×	✓	×	✓	✓	This system employs blockchain job scheduling to maintain the confidentiality of terminals, data, and identity inside a network.	Permits fog elements for performing cloud tasks at the edges of a system
Esposito, Ficco, Gupta [53]	2021	✓	✓	×	×	✓	Uses blockchain technology to obtain identity policies for operating in a global view of a distributed system	Distributed authorisation for operating the security policies within the system
Oham et al. [54]	2021	✓	✓	×	×	✓	Blockchain-based design for safeguarding vehicles	Aims to accomplish safety for vehicles
Xu et al. [55]	2021	✓	✓	×	✓	✓	Analytical model in blockchain for one and more networks	Obtains the average transaction latency
Chiang et al. [56]	2020	✓	✓	×	✓	✓	It uses a pseudo-random number generator and avoids double-spending	Using blockchain framework, discovered cryptocurrency for financial transaction
Hardin and Lotz [57]	2020	×	✓	×	✓	✓	Uses blockchain benefits in the healthcare system	Obtains the origin of information in health data
Liu et al. [58]	2020	✓	✓	×	✓	✓	Use of blockchain technology and space-structured ledger	Designed for heterogeneous IoT devices
Li, Wu, Jiang and Srikanthan [59]	2020	×	✓	×	✓	✓	Blockchain techniques for big data	Verification of integrity in cloud storage
Zhao et al. [60]	2020	✓	✓	×	✓	✓	Iot management systems using blockchain technology	It does not involve a trusted third-party
Liu, Wang, Lin, and Xu [61]	2019	×	✓	×	✓	✓	Reduced power usage using the blockchain mechanism	Designed for industrial IoT environments
Xu et al. [62]	2018	✓	×	×	✓	×	Big data application	Sharing over restricted edges
Abura'ed et al. [63]	2017	✓	×	✓	✓	×	Multichannel representation for quantum images uses 12 qubits for image encoding, and probability spreading is obtained using seven quantum measurements.	Works for multicolour images
Ruan et al. [64]	2016	✓	×	✓	✓	✓	Uses quantum techniques	Image classification using quantum devices
Zhang et al. [65]	2015	✓	×	✓	✓	×	Uses quantum feature extraction framework	Local feature extraction on quantum systems
Iliyasu et al. [66]	2011	✓	×	✓	✓	✓	Maintains an entangled two-dimensional qubit sequence for processing images using quantum techniques	A quantum state is created by applying a tensor product for integrating the colour and location of an image pixel-by-pixel
Andraca and Ball [67]	2010	×	×	✓	✓	×	Uses maximally entangled states to store points	Image segmentation using quantum systems
Latorre [68]	2005	×	×	✓	✓	✓	Uses image quartering	Constructs a stable quadtree table for greyscale pictures

Note: A. Framework B. Cryptography C. Image Processing D. Algorithms E. Performance evaluation.

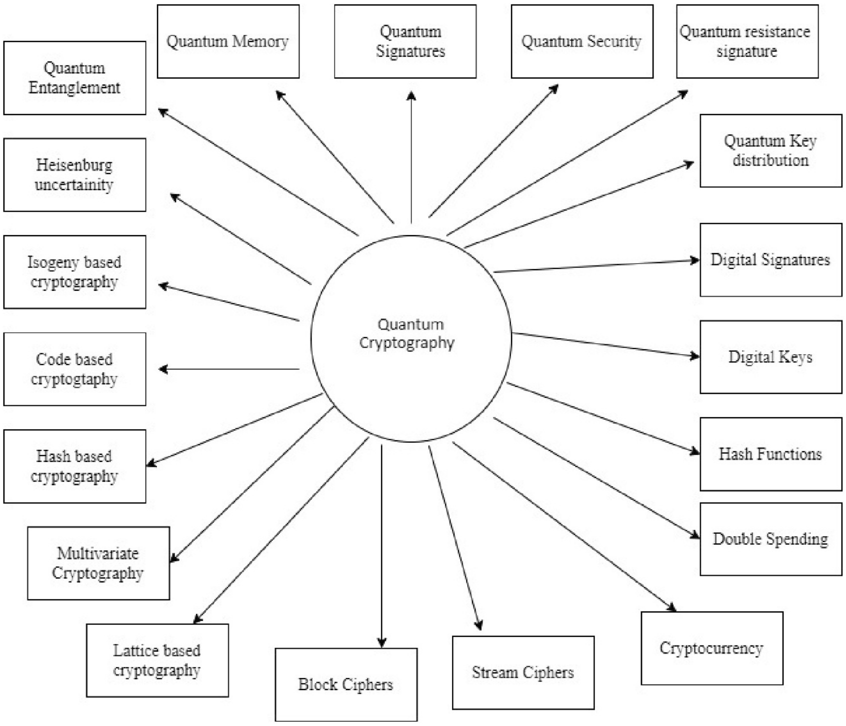


FIGURE 11 Quantum cryptography key terms.

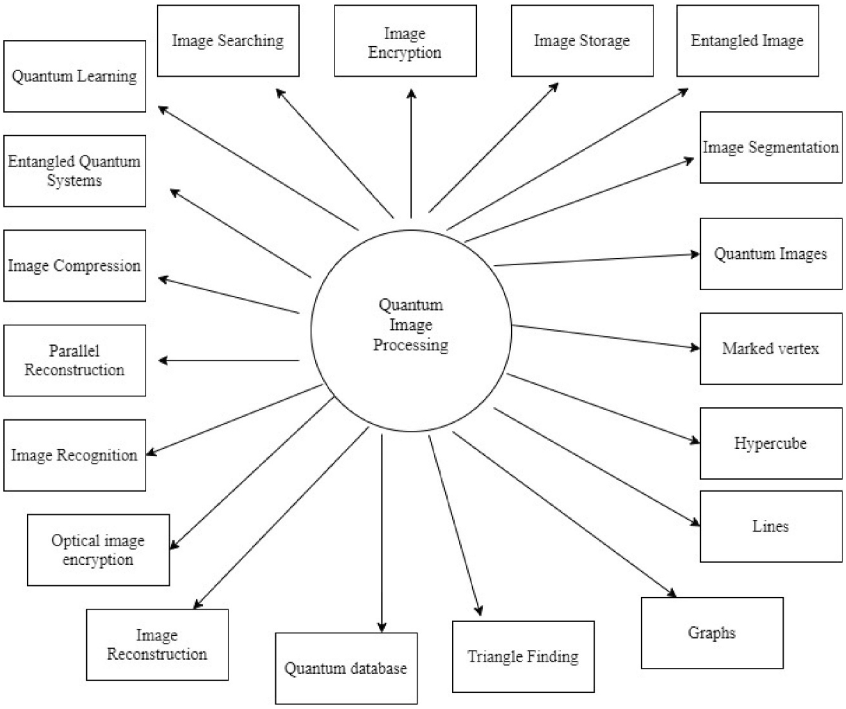


FIGURE 12 Quantum image processing key terms.

8 | QUANTUM BLOCKCHAIN APPLICATIONS

The application of blockchain technology spans many fields, encompassing post-quantum cryptography, quantum attack-resistant blockchains, cybersecurity, data management, and the advancement of intelligent societies. One of its most notable applications is cryptocurrency. Blockchain technology extends its influence across finance, healthcare, the Internet of Things, and cybersecurity. Z. Yang et al. [69] introduce blockchain-based identity management, where digital identities are created and utilised to authenticate users across different applications.

The 6G network harnesses advanced machine learning technology and has garnered significant attention. However, achieving superior performance in 6G technology faces scalability, massive connectivity, and trust issues. Consequently, future network technologies are trending towards distributed and decentralised ledger technologies like blockchain. The safety of blockchain technology depends on the computational difficulty of resolving scientific complications. Nevertheless, quantum computers possess the fundamental capacity to decipher such difficulties by their computing powers readily. Saini R. et al. [70] suggested a novel architecture that syndicates quantum blockchain expertise with 6G networks. Highly entangled quantum bit circuits (QBC) consisting of five, six, and seven qubits are employed to build the reversible circuits of the system. Using circuit optimisation, they apply mitigation techniques and do efficiency studies to showcase the benefits of error extenuation methods in maintaining the integrity of quantum bit circuits and running them on quantum hardware. Their research introduces quantum algorithms for smart contracts built on blockchain targeted at cloud-centric Internet of Things (IoT) applications. The development of related quantum circuits complements these algorithms. Potential results from these circuits are validated by evaluating input transaction data.

Health records in electronic format store extremely sensitive and secret data. Blockchain technology provides a secure way to transmit these documents to medical institutions. In their study, Z. Qu et al. [71] provided an innovative dispersed quantum automated medical record-based system and introduced a secure remote quantum blockchain system. This blockchain's facts format facilitates the interconnection of blocks using entangled states, minimising the necessary storage space by establishing control over quantum blocks. Per the quantum electronic medical record system, each block's hash value is saved using a single qubit through quantum information processing. The proposed methodology guarantees the protection and privacy of automated medical records within the framework of the Internet of medical belongings, therefore enabling the monitoring of individual medical data. The technique departs from conventional encryption and algorithmic digital signatures. Among the quantum computer assaults, entanglement measurement attacks, peripheral attacks and intercept-measure-repeat attacks are among the ones in the quantum blockchain network that offer strong stability. A comprehensive examination of the exactness and traceability of the quantum blocks is included in the paper along with circuit designs for calculating hash values.

The inherent characteristics of transparency and redundancy make blockchain and other distributed ledger technologies (DLTs) increasingly relevant in an extensive variety of uses. In the context of blockchain, these characteristics are enabled by protocols like public key cryptography and hash-based functions. Nevertheless, the emergence of quantum attacks, which exploit algorithms like Grover's search algorithm and factorisation algorithm of Shor, presents a profound menace to existing cryptographic techniques. T. M. Fernandes-Carames et al. [72] thoroughly analyse the current state of post-quantum cryptosystems and their possible uses in blockchains and distributed ledger technologies (DLTs). A comprehensive analysis assesses the features and effectiveness of utmost encouraging post-quantum public key encryption and digital signature systems appropriate for blockchain contexts.

The wide-ranging nature of blockchain technology has led to a need for standardised guidelines for developing blockchain applications. In their study, Y. Zeng et al. [73] introduced a feature-oriented categorisation method specifically designed for blockchain applications. This methodology examines and compares existing standard blockchain applications and frameworks, including digital currency blockchains, development platform blockchains, decentralised applications, and extended blockchains. The main goal is to help developers design blockchain applications in a focused way by clarifying the functional architectural aspects of various blockchain applications.

The field of blockchain technology has undergone swift advancement and is currently extensively employed in several industries, such as medicine, finance, and energy. Yet, as blockchain applications grow, they frequently function as segregated ecosystems where transactions and functions are limited to certain chains. This phenomenon has resulted in the proliferation of disparate and autonomous blockchains. Facilitating cross-chain connections, allowing cross-organisational data exchange, and expanding over numerous blockchains present significant challenges. Furthermore, quantum assaults present a substantial risk to blockchain data security. The blockchain smart contract approach proposed by X. Zheng et al. [74] aims to provide resistance against quantum computing threats. The methodology incorporates lattice cipher digital signatures within the blockchain framework to effectively counter quantum search process outbreaks.

Moreover, by implementing a keen agreement authentication system, nodes from several diverse chains are arranged into a peer-to-peer (P2P) system named identity agent layer. The purpose of this network is to enable chain transactions and ensure the establishment of reliable system and message verification systems among the chains. The proficiency of the algorithm is assessed through simulations of Bitcoin transaction scenarios and examination of empirical data. The extensive implementation of blockchain technology in many industries may be attributed to its decentralisation and transparency concepts. Nevertheless, the use of traditional cryptographic primitives that rely on enormous prime statistics or elliptic curves through logarithms is a notable obstacle in the era of quantum computing, as these rules become susceptible to attacks. To cope with the change during the pre-quantum to the post-quantum period, it becomes imperative to develop new cryptographic methods resistant to quantum assaults. In their study, R. Saha et al. [75] present a proposed approach to attain post-quantum decentralisation within blockchain networks. Their methodology employs frameworks using polynomials aimed at encryption built on identification and aggregate monograms for agreement, guaranteeing effectiveness and also appropriateness for post-quantum blockchain uses. To illustrate the usefulness of the suggested solution in tackling the issues presented by quantum computing vulnerabilities, it is evaluated based on parameters like complexity, delay, energy consumption and throughput.

The authors Naik et al. [76] present a complete summary of the up-to-date progress in quantum finance, including domains such as fraud detection, portfolio optimisation, and the utilisation of Monte Carlo techniques for derived rating and risk evaluation. Additionally, the study explores incorporating quantum computing with blockchain technology, a fundamental aspect of financial technology (fintech). A comprehensive analysis of blockchain centres on its core cryptographic primitives, including algorithms for digital signatures, hash functions, and generators of random numbers. Considering the advent of quantum computers, the discussion underscores the weaknesses of blockchain technologies. This work investigates privacy-preserving methods in quantum-resistant blockchain schemes, such as zero-knowledge proof systems, threshold signatures and ring signatures. The text underscores the differentiation between blockchains resistant to quantum attacks and those that are secure against them while also delineating the necessary security protocols to be adopted.

Three security concepts have been proposed by S. Mahapatra et al. [77] to improve the robustness of blockchain systems against quantum computing. These systems tackle crucial domains like as the protected distribution of healthcare data, polling processes, international expenditures, protection of individual identification, and exchanges of cryptocurrencies, all positioned to revolutionise information management methods radically. Advancements in technology have recently increased concerns over the susceptibility of data to quantum attacks. Insufficient measures to safeguard privacy in blockchain systems can jeopardise substantial amounts of user data, highlighting the pressing requirement for strong privacy-preserving techniques resistant to quantum computing capabilities. The first security approach suggested entails using classical-quantum mappings to establish zero-knowledge guarantees for data secrecy. To improve information security within a double random phase encoding framework, the second strategy presents an optical encryption technique that provides greater complexity and resistance in the Fresnel domain. Furthermore, the third method utilises a wavelet-based steganography technique to improve the storage, hiding, and restrictions on accessing data. This approach utilises the wavelet realm to include pseudo-quantum indications into red, green, blue colour QR codes, therefore enhancing encryption capabilities and guaranteeing strong security protocols. Using cryptographic tools, blockchain technology offers secure solutions for diverse online activities. M. Buser et al. [78] surveyed the current literature on post-quantum secure digital signatures, essential cryptographic tools within the blockchain ecosystem. These signatures are critical in enhancing consensus efficiency, managing accounts, enabling script-less blockchain operations, and ensuring privacy. The paper focuses on several specialised types of signatures, including multi-aggregate, threshold, adapter, blind, and ring signatures. These signatures are categorised as "exotic" due to their novel functionalities and advanced features. The survey includes in-depth discussions on existing challenges associated with these signatures and proposes future research directions to advance their security and applicability in blockchain technologies.

The applications of quantum blockchain technology are diverse and span several key industries. Each benefits from the enhanced security and efficiency offered by quantum cryptographic methods.

1. Finance and Cryptocurrencies

Blockchain technology revolutionises transaction processing, recording, and verification in the financial sector. However, the rise of quantum computing looms over the cryptographic foundations of these schemes, particularly the public-key cryptography used to protect digital wallets and dealings. Quantum blockchain technology can report these vulnerabilities by implementing quantum-resistant cryptographic procedures, like lattice-based signatures, ensuring that transactions remain secure despite quantum attacks.

One potential application is in the development of quantum-secure cryptocurrencies. These digital currencies would leverage quantum blockchain protocols to ensure that all transactions are immutable, transparent, and resistant to quantum decryption. Additionally, quantum-resistant consensus devices, such as quantum delegated proof of stake (QDPoS), could secure blockchain networks without relying on energy-intensive processes such as traditional proof of work (PoW).

2. Healthcare and Electronic Medical Records (EMRs)

The healthcare industry relies heavily on managing secure, confidential electronic healthcare records (EMR). It has been suggested that blockchain technology can guarantee privacy and data integrity in the medical field. Still, the encryption techniques currently in use to safeguard EMRs are seriously threatened by quantum computing.

Quantum blockchain technology can offer a robust solution by integrating quantum key distribution (QKD) protocols with blockchain frameworks. This would ensure that the encryption keys to secure patient data are immune to quantum attacks. Furthermore, quantum-secure smart contracts could manage access to medical records, ensuring only authorised personnel can view or modify patient information.

In addition, quantum blockchain systems could facilitate protected and efficient record distribution among medical providers, improving collaboration and patient outcomes while maintaining the highest data privacy and security standards.

3. Internet of Things (IoT) and Smart Cities

The Internet of Things (IoT) connects billions of devices worldwide, permitting to communicate and share information. However, the security of IoT networks is a significant concern, particularly as these devices often work in situations with inadequate computational properties. Blockchain technology can enhance IoT security through a decentralised and tamper-proof record for information storage and device communication.

Quantum blockchain can take this a step further by implementing quantum-resistant cryptographic protocols tailored to the needs of IoT devices. For instance, quantum-safe identity management systems could ensure that only trusted devices can join and communicate within an IoT network. Additionally, quantum blockchain could support secure and scalable data management in keen capitals, who have huge volumes of records which are continuously created and shared across various systems.

In smart city applications, quantum blockchain could enable secure data transactions for energy management, transportation, and public safety. By integrating quantum cryptographic methods, these systems can protect sensitive data from being intercepted or altered by quantum-capable adversaries.

9 | CHALLENGES, ISSUES, LIMITATIONS, AND POSSIBLE SOLUTIONS

Quantum methods such as Shor's factorising algorithm, which performs factorisation on big numbers, and Grover's search algorithm, working for exploring unstructured databases, provide exponential and quadratic increases in speed compared to classical methodologies. These technological developments provide substantial risks to public key cryptosystems and hash functions, leading to a transition towards quantum-secure cryptography. Kiktenko et al. [79] examines the present and potential advancements in the scalability and security of the blockchain architecture. The evaluation examines projects concentrating on quantum-safe blockchain cryptosystems by comparing measurements of hash dimensions, hash lengths, performance times, energy efficiency, and computational overhead. The study objective is to investigate the potential of quantum-enhanced solutions in addressing the obstacles encountered in blockchain technology to improve its scalability, security, and performance.

Since the onset of the pandemic, there has been a surge in online personal transactions, highlighting the critical importance of privacy in data protection regulations. This trend has underscored the necessity for systems that comply with privacy regulations and effectively resist attacks. A comprehensive examination of blockchain technology reveals several challenges, including issues with user identity, transaction linkability, and cryptographic key management. It is crucial to scrutinise vulnerabilities at each layer of the blockchain architecture.

S. Bansod and Ragha [80] investigate the evolution of several privacy-enhancing technologies, including zero-knowledge proofs (ZKPs), ring signatures, secure multi-party computation (SMPC), mixing services, homomorphic encryption, and quantum-resistant computing. Furthermore, the authors assess the privacy-enhancing measures adopted by blockchain systems such as ZCash, Zerocoin, Hyperledger, and Wanchain. Kiktenko et al. [79] proposed a protocol for protecting blockchains when an attack is made using a quantum computer and have verified their protocol experimentally. Four nodes in the protocol called W, X, Y, and Z are linked using a network, as shown in Figure 13(a).

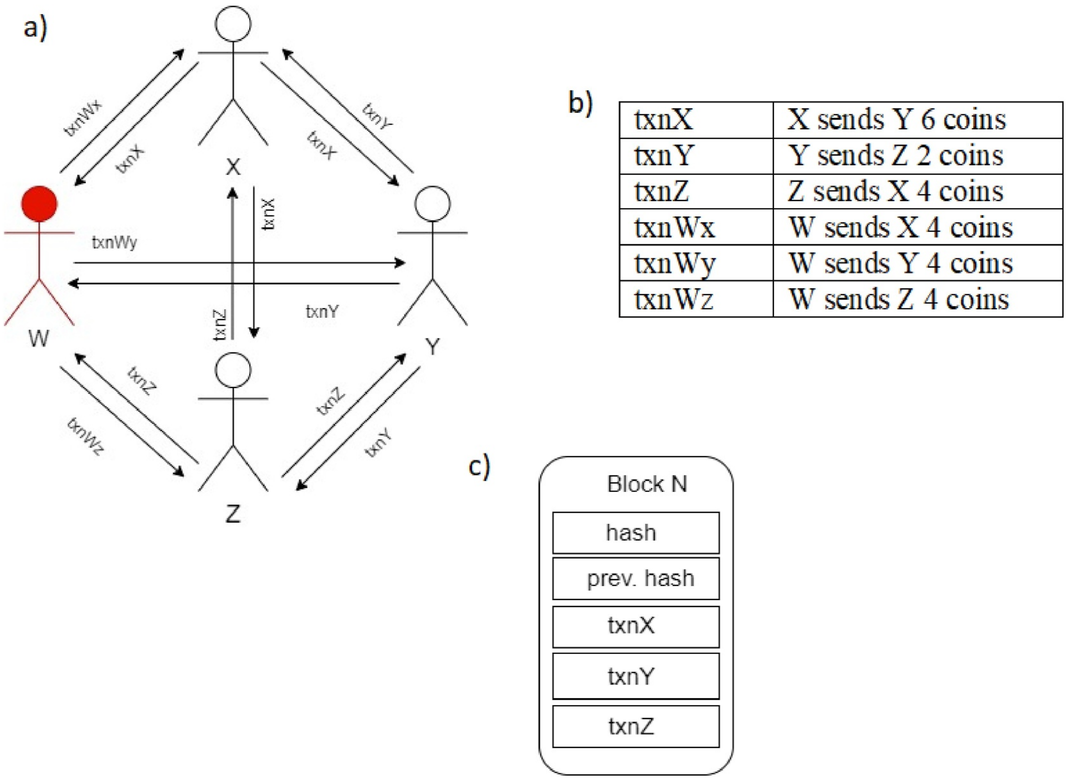
The nodes X, Y, and Z perform valid transactions, and W uses the same transaction multiple times, hence performing double-spending. At each node, a collection of unconfirmed transactions consisting of three valid and one invalid transaction is formed. The broadcast protocol is then applied to these transaction pools. After the second round, the protocol removes the W's invalid transactions and creates a block containing only valid transactions.

Nodes X, Y, and Z are interested in making valid transactions, denoted as txnX, txnY, and txnZ. They send the same copies of their transaction to all other nodes. Node W is going to make an invalid transaction, sending non-identical versions txnWx, txnWy, and txnWz of the same transaction to different nodes as shown in Figure 13(a). Transaction contents are shown in Figure 13(b) and the broadcast protocol is implemented at each node to resolve the unconfirmed transactions and a block is constructed. They find that the transaction initiated by node W is invalid and eliminate it as shown in Figure 13(c).

Ahmed et al. [81] have introduced an encryption protocol leveraging quantum walks. They proposed a blockchain framework designed to transmit information between IoT devices securely. In this blockchain, blocks are interconnected using quantum hash functions. The authors illustrated that this approach enables successful data transmission among devices, effectively safeguarding against attacks and enabling seamless information sharing with other nodes. Sun et al. [82] introduced LogiContract (LC), a blockchain system incorporating quantum protection. The researchers employed a digital signature pattern that utilised quantum key distribution techniques and a consensus mechanism built around voting to establish acceptance on the blockchain. The authors presented a scalable consensus mechanism and a secure signing technique for LogiContract, specifically developed to counteract the risks posed by quantum computer assaults.

Quantum blockchain by entanglement in period has been designed by Rajan and Visser [83]. The authors have replaced the traditional chain with a quantum scheme. The idea of the chain is obtained through the entanglement of photons. The data structures in classical blockchain work using time-stamped chunks and using hash jobs based on cryptography are linked sequentially. When an invader interferes with a specific chunk, all future chunks following the interfered chunk are cancelled. Therefore, the portions next to the disrupted block are demolished owing to cryptographic mix up operations, thereby leaving them vulnerable to errors.

Jiaxing et al. [84] devised a blockchain method to securely audit different application credentials to improve data security. Their methodology minimises communication and automation costs by removing the need for third-party auditors. Three primary entities are involved in this approach: the data owner, the public auditor, and the provider of the cloud service.



txnX	X sends Y 6 coins
txnY	Y sends Z 2 coins
txnZ	Z sends X 4 coins
txnWx	W sends X 4 coins
txnWy	W sends Y 4 coins
txnWz	W sends Z 4 coins

FIGURE 13 Block creation in a quantum-secure blockchain.

Originally, the data owner partitions the file into segments, applies encryption, and produces tags by a hash operation. After that, a Merkle Hash Tree (MHT) is generated, and the data owner preserves the root of the MHT. Accordingly, the files belonging to the data owner are retained in the cloud, and the blockchain contains the associated tags. Subsequently, the data owner chooses a public auditor for the blockchain network. The public auditor constructs a metrics and audit trail (MHT) by utilising the tags obtained from the blockchain and transmits evidence to the data owner. Following that, the data owner initiates a challenge to the cloud service provider, who then replies with a mapped hash table (MHT) that includes the tags of the blocks belonging to the data owner. The data owner authenticates the findings presented by the public auditor and cloud service provider to guarantee the correctness and dependability of its record.

Bassem et al. [85] have introduced an encryption method leveraging quantum walks. Their protocol involves employing alternating quantum walks across two stages. Quantum walks are integrated into optical image encryption frameworks. The effectiveness of their technique is verified through simulations, including analysis of correlations, histograms, sensitivity, key space, noise, and data loss. These analyses aim to uncover and identify potential uses of quantum techniques in enhancing the safety of the information.

Ahmed et al. [86] have suggested a technique for securing patient data through two algorithms designed for image encryption and decryption. These algorithms utilise a substitution and permutation process with controlled alternate quantum walks. The authors conducted simulations to validate the effectiveness and safety of their image encryption algorithm. The encryption algorithm begins by capturing the original image dimensions (height, width, and colour) and storing them in a matrix denoted as P. Using initial values for the substitution process and employing quantum walks, a matrix KP is constructed, which is then converted into numerical standards ranging from 0 to 255 to generate a key sequence K. The substituted image S is obtained by performing an operation of BitXOR between the original images K and G. Subsequently, using initial values for the permutation process, a probability matrix P is derived and resized to match the dimensions of the image G, stored as matrix X. Matrix X is sorted in ascending order to produce vector Y, where each element's index in X is stored as vector Z to calculate the permuted image. The encrypted image is obtained by applying permutation to the substituted image using vector Z. The decryption algorithm reverses the steps of the encryption algorithm. Initially, it retrieves the size of the encrypted image, applies the permutation process and controlled alternate quantum walks to obtain matrix X, rearranges its values from smallest to largest, and calculates vector Z by finding the indices of each component in vector Y. Permutation is then applied to the encrypted image using vector Z. Using initial values for the substitution process and executing controlled alternate quantum walks, the probability condition P is derived, resized to match the length of the permuted image, and stored as KP. KP is converted into integer standards in the range of 0–255, stored in a variable K, and a BitXOR operation is performed between matrix K and the permuted image to obtain the decrypted image.

The next generation of innovation is represented by blockchain technology, which has applications in supply chain management, identity management, smart contracts, cryptocurrencies, and cross-border payments. Major advantage of blockchain is its decentralised nature, where control is distributed among its users rather than centralised authorities. Beyond its original use in cryptocurrencies, blockchain is now understood as a straightforward concept rather than a complex one due to its expanding applications. Verification, decentralisation, fault tolerance, immutability, integrity, fault tolerance, transparency and anonymity are some of the desired properties of blockchain technology. Habib et al. [87] provide a comprehensive analysis of blockchain technology, covering its evolution, various applications, benefits, cryptographic specifics, and challenges in distributed transaction ledgers. It offers an in-depth assessment of blockchain technology, addresses serious tasks, and explores its uses across diverse domains. The paper also delves into the specifics of various cryptocurrencies associated with blockchain technology.

Quantum computing harnesses entanglement, superposition, and other fundamental principles to tackle complex problems further than the abilities of classical systems. Recent years have seen significant strides in unravelling the intricacies of quantum computing. S.S. Gill [88] explores the initial values and prospects of quantum computing based on current research. The paper delves into cutting-edge advancements in quantum hardware, as well as subsequent progress in quantum cryptography and software development. It also identifies potential challenges and emerging trends in the growth of quantum technologies.

A thorough review and analysis of the present situation, difficulties, and future possibilities of post-quantum cryptography are given by Horpenyuk et al. [89]. The paper looks at post-quantum cryptography standardisation initiatives by institutions like the National Institute of Standards and Technology (NIST). It highlights the key sizes and implementations of different post-quantum cryptography algorithms and classifies and describes their essential characteristics. Furthermore, the paper discusses the development of open-source libraries like open quantum safe, which offer practical implementations of diverse post-quantum algorithms. It emphasises the importance of getting ready for the quantum computing age as awareness of its importance grows. Many businesses, institutions, and governmental bodies are evaluating how quantum computing will affect their data security and infrastructure.

Quantum communication transforms secure data transmission through quantum physics to mitigate encryption vulnerabilities. It harnesses quantum phenomena such as the superposition of states and quantum entanglement, rendering handling efforts measurable for unparalleled security. Global quantum communication networks are complex to establish; therefore, new developments in signal detection, quantum repeaters and storage are required. Q. H. Abbasi et al. [90] outline future trends focusing on refining methodologies to enhance efficiency and substantially improve secure protocols and network performance.

Blockchain is a unique computer data structure that provides an open, distributed and public ledger with many potential uses. Any new application involving cryptography should consider expected technical advancements that will take place during the system's deployment. B. Rodenberg et al. [91] assess vulnerabilities in blockchain technology due to the advent of quantum computers and provide general recommendations on enhancing blockchain's resilience against technological advancements.

10 | CONCLUSION AND OPEN QUESTIONS

Research in the field of quantum blockchain is focused on developing quantum-resistant and quantum-enhanced security measures. Traditional blockchains rely on hashing and asymmetric cryptography, which are susceptible to Shor's algorithm —a quantum algorithm capable of solving integer factorisation and discrete logarithm problems exponentially faster than classical computers. To mitigate these risks, researchers are investigating post-quantum cryptographic (PQC) solutions and innovative quantum mechanisms to fortify blockchain structures.

The method in which we handle data is revolutionised by blockchain technology, especially in terms of content integrity and transparency. Quantum computing, on the other hand, presents certain difficulties for the cryptographic underpinnings of traditional blockchain systems. Our research focuses on a new era of quantum blockchains that can reduce risks by implementing post-quantum cryptography solutions. The blockchain community has faced its most horrific threat due to the rise of quantum computing.

In this overview of quantum-resistant systems, including lattices-based, multivariate polynomial cryptography and hash-based, we can see how they can strengthen blockchain networks against the impact of future attacks from quantum computers. We have also highlighted the various use cases of quantum blockchain in industries such as finance, healthcare and IoT, thus demonstrating how it can disrupt those sectors profoundly by taking them to an even greater degree of security and efficiency. The future of the next generation is bright, as blockchain will be rapidly integrated into quantum computing. Quantum-resistant blockchain systems will motivate an important role in guaranteeing the safety and trustworthiness of decentralised networks as research progresses. This promising integration of quantum computing with blockchain will secure critical infrastructure, improve data privacy, and revolutionise data management, offering a hopeful future for the technology.

The entire community must engage in further investigation and design of quantum-secure blockchain protocols. This includes addressing issues around scalability and integration with existing systems and, most importantly, implementing quantum cryptographic solutions. This collective effort will ensure that blockchain maintains its fortitude as a secure technology, immune from the threats an expansion of quantum would bring about in the age of ubiquitous qubits. The decentralised and immutable nature of blockchain technology has brought about a fundamental transformation in the data integrity and security standards across various industries, including retail, energy, and banking. However, the advent of quantum computing poses significant threats to the security of traditional blockchain systems, necessitating advancements in quantum blockchain technology. This emerging field leverages quantum computation and cryptography to enhance blockchain's resilience against quantum attacks, ensuring robust security for applications like online transactions, digital banking, and the Internet of Vehicles (IoV).

Integrating quantum principles into blockchain technology substantially improves authentication protocols and encryption mechanisms. Quantum key distribution, quantum digital signatures, and lattice-based cryptography provide stronger defenses against cyber threats, making them suitable for dynamic environments such as vehicular networks and industrial IoT systems. Additionally, quantum blockchain frameworks promise superior energy efficiency, data computation, and key storage performance compared to classical methods. Moreover, research into quantum walks underscores their potential applications in cryptography and image processing. They are showcasing accelerated problem-solving abilities and heightened data security. The investigation into quantum-secure digital currencies, smart contracts, and decentralised ledgers underscores how quantum technologies can revolutionise blockchain systems.

Without question, the combination of blockchain technology and quantum computing marks a significant breakthrough in cybersecurity. Quantum blockchain-based authentication methodologies and cryptographic algorithms are essential for strengthening key infrastructures against emerging cyber threats, guaranteeing secure communication, and maintaining data integrity in various uses, including healthcare and big data management. The continuous endeavours to create and implement designs resistant to quantum cryptography will be crucial in addressing the difficulties presented by quantum threats and improving the general safety of blockchain networks.

Quantum blockchain is an emerging field that combines the principles of quantum computing and blockchain technology. However, it is still in its infancy, and there are many open research questions that need to be addressed before widespread adoption. Some key open questions are as follows:

- Which quantum-resistant algorithms are most suitable for blockchain integration?
- How can these algorithms be optimised for performance, scalability and energy efficiency in blockchain applications?
- Can quantum blockchain support large-scale decentralised applications with high transaction volumes?
- How can quantum and classical blockchains interoperate in a seamless and secure manner?
- What mitigation strategies can be applied in the short term to safeguard classical blockchains until quantum-resistant solutions are in place?
- What will the transaction process look like for industries relying on classical blockchains to move to quantum blockchains?
- How will users, developers, and enterprises prepare for this shift, and what tools or support will be needed?

Addressing these questions will be essential to fully realise the potential of quantum blockchain and ensure its secure and efficient implementation in the future.

AUTHOR CONTRIBUTIONS

Manjula Gandhi S: Conceptualisation; Data curation; Investigation; Methodology; Validation; Writing - original draft; Writing - review & editing. **Jafar Ali Ibrahim Syed Masood**: Conceptualisation; Formal analysis; Investigation; Project administration; Resources; Supervision; Validation; Visualisation; Writing - original draft; Writing - review & editing. **Chaitrali Mulay**: Formal analysis; Resources; Software; Validation. **Karthiganesh Durai**: Software. **G Murali**: Supervision. **Vijayarajan V**: Conceptualisation; Writing - review & editing. **Kumar Gautam**: Validation. **N. S. Kalyan Chakravarthy**: Data curation; Formal analysis; Investigation; Methodology; Supervision; Visualisation. **S. Suresh Kumar**: Investigation. **Saurabh Agarwal**: Software. **Murali S**: Methodology. **Vijayasherly V**: Project administration. **David Asirvatham**: Visualisation. **Sarfraz Brohi**: Investigation. **Chandru Vignesh C**: Resources. **Anbuchelian S**: Resources; Software; Validation.

ACKNOWLEDGEMENTS

The authors have not received funding from any of the sources.

CONFLICT OF INTEREST STATEMENT

The work is not submitted to any other journal. There is no conflict of interest.

DATA AVAILABILITY STATEMENT

The dataset or information generated and/or analysed during the current study is available upon reasonable request from the corresponding author.

ORCID

Jafar Ali Ibrahim Syed Masood https://orcid.org/0000-0003-3076-5453
Kumar Gautam https://orcid.org/0000-0003-4387-7390

REFERENCES

1. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press (2010)
2. IBM Qiskit textbook.https://qiskit.org/textbook-beta/
3. David Mermin, N.: Quantum Computer Science, an Introduction. Cambridge University Press (2007)
4. Ezratty, O.: Understanding quantum technologies. (2021)

5. Wang, X., Xu, G., Yu, Y.: Lattice-based cryptography: a survey. Chin. Ann. Math. Ser. B 44(6), 945–960 (2023). https://doi.org/10.1007/s11401-023-0053-6
6. Bagchi, P., et al.: Public Blockchain envisioned security scheme using post quantum Lattice based aggregate signature for Internet of Drones Applications. IEEE Trans. Veh. Technol. 72(8), 10393–10408 (2023). https://doi.org/10.1109/tvt.2023.3260579
7. De Feo, L., Jao, D., Plût, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. J. Math. Cryptol. 8(3), 209–247 (2014). https://doi.org/10.1515/jmc-2012-0015
8. Hülsing, A., et al.: XMSS: eXtended Merkle signature scheme. RFC 8391 (2018)
9. Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: Post-quantum Cryptography, pp. 164–175. Springer (2020)
10. Misoczki, R., et al.: MDPC-McEliece: new McEliece variants from moderate density parity-check codes. In: 2013 IEEE International Symposium on Information Theory, pp. 2069–2073. IEEE (2013)
11. Wang, W., Yu, Y., Du, L.: Quantum Blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm. Natl. Libr. Med. 12(1), 8606 (2022). 21. https://doi.org/10.1038/s41598-022-12412-0
12. Sharma, P., et al.: Securing optical networks using quantum secured blockchain: an overview. Sensors 23(3), 1228 (2023). https://doi.org/10.3390/s23031228
13. Li, C.Y., et al.: A new lattice based signature scheme in the post quantum blockchain network. IEEE Access 7, 2026–2033 (2018). https://doi.org/10.1109/access.2018.2886554
14. Abd El Latif, A.A., et al.: Quantum inspired blockchain based cybersecurity:securing smart edge utilities in IoT based smart cities. Inf. Process. Manag. 58(4), 102549 (2021). https://doi.org/10.1016/j.ipm.2021.102549
15. Allende, M. et al.: Quantum Resistance in blockchain networks. Sci. Rep. 13(1), 5664, https://doi.org/10.1038/s41598-023-32701-6, Article number 5664, (2023)
16. Selvarajan, S., Mouratidis, H.: A quantum trust and consultative transaction based blockchain cybersecurity model for health care systems. Sci. Rep. 13(1), 7107 (2023). Article number 7107, May. https://doi.org/10.1038/s41598-023-34354-x
17. Makwana, B., et al.: Blockchain and quantum blind signature based hybrid scheme for health care 5.0 applications. J. Inf. Secur. Appl. 56, 102673 (2021). https://doi.org/10.1016/j.jisa.2020.102673
18. Holcomb, A., et al.: PQFabric: a permissioned blockchain secure from both classical and quantum attacks. Computer Sci. -Cryptography security 3 (2020)
19. Zhang, P., et al.: A Blockchain system based on quantum resistant digital signature. Secur. Commun. Network. 2021, 1–13 (2021). https://doi.org/10.1155/2021/6671648
20. Sagar Gupta, D., et al.: Quantum-defended blockchain-assisted data authentication protocol for internet of vehicles. IEEE Trans. Veh. Technol. 71(1), 1–3266 (2022). 1. https://doi.org/10.1109/tvt.2022.3144785
21. Lu, R., et al.: Ecpp: efficient conditional privacy preservation protocol for secure vehicular communications. In: Proceedings of the 27th IEEE Conference on Computer Communication, Phoenix, AZ, USA (2008)
22. Sagar Gupta, D., Biswas, G.P.: A novel and efficient lattice-based authenticated key exchange protocol in C-K Model. Int. J. Commun. Syst. 31(6), e3473 (2017). https://doi.org/10.1002/dac.3473
23. Mukherjee, S., Gupta, D.S., Biswas, G.: An efficient and batch verifiable conditional privacy preserving authentication scheme for vanets using lattice. Computing 101(12), 1763–1788 (2019). https://doi.org/10.1007/s00607-018-0689-3
24. Karati, A., Islam, S.H., Karuppiah, M.: Provably secure and lightweight certificateless signature scheme for IIoT environments. IEEE Trans. Ind. Inf. 14(8), 3701–3711 (2018). https://doi.org/10.1109/tii.2018.2794991
25. Su, S., et al.: A Reputation management scheme for efficient malicious vehicle identification over 5G Networks. IEEE Wireless Commun. 27(3), 46–52 (2020). https://doi.org/10.1109/mwc.001.1900456
26. Wang, X., et al.: An improved authentication scheme for internet of vehicles based on blockchain technology. IEEE Access 7(99), 1–45072 (2019). 1. https://doi.org/10.1109/access.2019.2909004
27. Suaib Akhter, A.F.M., et al.: A blockchain based authentication protocol for cooperative vehicular ad-hoc network. Sensors 21(4), 1273 (2021). February 2021. https://doi.org/10.3390/s21041273
28. Gawali, P., et al.: Quantum key distribution and blockchain based secure authentication in medical cyber-physical systems. Int. Conf. ICT Sustain. Dev., 607–622 (2023). https://doi.org/10.1007/978-981-99-6568-7_54
29. Gheorghies, A.-S., Lazaroi, D.-M., Simion, E.: A Comparative study of Cryptographic key Distribution protocols. (2021)
30. Gao, X., et al.: Practical randomized RLWE-based key exchange against signal leakage attack. IEEE Trans. Comput. 67(11), 1584–1593 (2018). https://doi.org/10.1109/tc.2018.2808527
31. Kumar, A., et al.: Revolutionizing modern networks: advances in AI, machine learning and blockchain for quantum satellites and UAV based communication. (2023)
32. Norouzzadeh, M.S., et al.: Automatically identifying, counting and describing wild animals in camera trap images with deep learning. Biol. Sci. 115(25), E5716–E5725 (2018). https://doi.org/10.1073/pnas.1719367115
33. Shaikh, T.A., Ali, R.: Quantum computing in big data analytics: a survey. In: IEEE International Conference on Computer and Information Technology, pp. 112–115 (2017)
34. Dai, W.: Quantum Computing with AI and Blockchain: modelling, fault tolerance and capacity scheduling. Math. Comput. Model. Dyn. Syst. 25(6), 523–559 (2019). https://doi.org/10.1080/13873954.2019.1677725
35. Yuan, B., et al.: Blockchain based infrastructure for artificial intelligence with quantum resistant. In: 4th International Conference on Artificial Intelligence and Big Data (2021)
36. Kaushik, K., Kumar, A.: Demystifying quantum blockchain for healthcare. 6(3), https://doi.org/10.1002/spy2.284 (2022)
37. Singh, M., et al.: Quantum artificial intelligence for the science of climate change. arxiv:2108.10855, (2021)
38. Li, C., et al.: Quantum blockchain: a decentralized, encrypted and distributed database based on quantum mechanics. J. Quan. Comput. 1(2), 49–63 (2019). https://doi.org/10.32604/jqc.2019.06715
39. Sgantzos, K., Grigg, I.: Artificial intelligence implementations on the blockchain. Use cases and future applications. Blockchain: Curr. Challenges Future prospects/ Appl. 11(8), 170 (2019). https://doi.org/10.3390/fi11080170
40. How, M.L., Cheah, S.M.: Forging the future:strategic approaches to quantum AI integration for industry transformation. MDPI 5(1), 290–323 (2024). https://doi.org/10.3390/ai5010015
41. Kalafatic, K.: Using blockchain principles for improving AI research and security. (2018)
42. Ramos, S., Ellul, J.: Blockchain for Artificial Intelligence: enhancing compliance with the EU AI act through distributed ledger technology, A cybersecurity perspective. Int. cybersecurity L. Rev. 5, 1–20 (2024). https://doi.org/10.1365/s43439-023-00107-9
43. Rawat, B., et al.: Quantum computing and AI: impacts and possibilities. ADI J. Recent Innovation 3(2), 202–207 (2022). https://doi.org/10.34306/ajri.v3i2.656
44. Jones, C.: "AI, Big Data, Quantum Computing and Financial Exclusion: Tempering Enthusiasm and Offering a Human Centric Approach to Policy", Fintech, Artificial Intelligence and the Law: Regulation and Crime Prevention, pp. 193–210. Financial Crime series, London (2021)
45. Bonab, A.B., et al.: Urban Quantum Leap: a comprehensive review and analysis of quantum technologies for smart cities. Cities 140, 104459 (2023). https://doi.org/10.1016/j.cities.2023.104459
46. Hasanova, H., et al.: A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. Int. J. Netw. Manag. 29(2), e2060 (2019). https://doi.org/10.1002/nem.2060
47. Aharonov, Y., Davidovich, L., Zagury, N.: Quantum random walks. Phys. Rev. A. 48(2), 1687–1690 (1993). https://doi.org/10.1103/physreva.48.1687

48. Magniez, F., Santha, M., Szegedy, M.: Quantum algorithms for the triangle problem. SIAM J. Comput. 37(2), 413–424 (2007). https://doi.org/10.1137/050643684
49. Kendon, V., Sanders, B.: Complementarity and quantum walks. Phys. Rev. A. 71(2), 022307 (2005). https://doi.org/10.1103/physreva.71.022307
50. Chrzastek, Z.: Assessment of IBM-Q Quantum Computer and its Software Environment. Master's Thesis, AGH University of Science and Technology (2018)
51. IBM quantum experience https://quantum-computing.ibm.com/
52. Baniata, H., Anaqreh, A., Kertesz, A.: PF-BTS: a privacy-aware fog-enhanced blockchain-assisted task scheduling. Inf. Process. Manag. 58(1), 102393 (2021). https://doi.org/10.1016/j.ipm.2020.102393
53. Esposito, C., Ficco, M., Gupta, B.B.: Blockchain-based authentication and authorization for smart city applications. Inf. Process. Manag. 58(2), 102468 (2021). https://doi.org/10.1016/j.ipm.2020.102468
54. Oham, C., et al.: B-FERL: blockchain based framework for securing smart vehicles. Inf. Process. Manag. 58(1), 102426 (2021). https://doi.org/10.1016/j.ipm.2020.102426
55. Xu, X., et al.: Latency performance modeling and analysis for hyperledger fabric blockchain network. Inf. Process. Manag. 58(1), 102436 (2021). https://doi.org/10.1016/j.ipm.2020.102436
56. Chiang, C.-Fu, et al.: A quantum assisted secure client-centric polyvalent blockchain architecture for smart cities. In: 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), IEEE, pp. 1–6 (2020)
57. Hardin, T., Kotz, D.: Amanuensis: information provenance for health-data systems. Inf. Process. Manag. 58(2), 102460 (2020). https://doi.org/10.1016/j.ipm.2020.102460
58. Liu, Y., et al.: Tornado: enabling blockchain in heterogeneous Internet of Things through a space-structured approach. IEEE Internet Things J. 7(2), 1273–1286 (2020). https://doi.org/10.1109/jiot.2019.2954128
59. Li, J., et al.: Blockchain-based public auditing for big data in cloud storage. Inf. Process. Manag. 57(6), 102382 (2020). https://doi.org/10.1016/j.ipm.2020.102382
60. Zhao, Q., et al.: Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. Inf. Process. Manag. 57(6), 102355 (2020). https://doi.org/10.1016/j.ipm.2020.102355
61. Liu, Y., et al.: LightChain: a lightweight blockchain system for industrial internet of Things. IEEE Trans. Ind. Inf. 15(6), 3571–3581 (2019). https://doi.org/10.1109/tii.2019.2904049
62. Xu, C., et al.: Making big data open in edges: a resource-efficient blockchain-based approach. IEEE Trans. Parallel Distr. Syst. 30(4), 870–882 (2018). https://doi.org/10.1109/tpds.2018.2871449
63. Abura'ed, N., Khan, F.S., Bhaskar, H.: Advances in the quantum theoretical approach to image processing applications. ACM Comput. Surv. 49(4), 1–49 (2017). https://doi.org/10.1145/3009965
64. Ruan, Y., et al.: Quantum computation for large-scale image classification. Quant. Inf. Process. 15(10), 4049–4069 (2016). https://doi.org/10.1007/s11128-016-1391-z
65. Zhang, Y., et al.: Local feature point extraction for quantum images. Quant. Inf. Process. 14(5), 1573–1588 (2015). https://doi.org/10.1007/s11128-014-0842-7
66. Le, P.Q., et al.: A flexible representation and invertible transformations for images on quantum computers. Stud. Comput. Intelligence 372, 179–202 (2011). https://doi.org/10.1007/978-3-642-11739-8_9
67. Venegas-Andraca, S.E., Ball, J.L.: Processing images in entangled quantum systems. Quant. Inf. Process. 9(1), 1–11 (2010). https://doi.org/10.1007/s11128-009-0123-z
68. Sharma, N., Gautam, K., Parthasarathy, H.: Estimating Hamiltonian fluctuations from quantum time averages. IET Quan. Commun. (Willy) 1(2), 62–71 (2020). https://doi.org/10.1049/iet-qtc.2020.0001
69. Yang, Z., et al.: Decentralization using Quantum Blockchain: a theoretical analysis. IEEE Trans. Quan. Eng. 3, 1–16 (2022). https://doi.org/10.1109/tqe.2022.3207111
70. Saini, R., et al.: Designing Quantum Blockchain system integrated with 6G network. J. King Saud University- Comput. Inf. Sci. 35(10), 101847 (2023). https://doi.org/10.1016/j.jksuci.2023.101847
71. Qu, Z., Zhang, Z., Zheng, M.: A quantum blockchain enabled framework for secure private electronic medical records in Internet of Medical Things. Inf. Sci. 612, 942–958 (2022). https://doi.org/10.1016/j.ins.2022.09.028
72. Fernandes- Carames, T.M., Fraga- Lamas, P.: Towards post quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks. IEEE Access 8, 21091–21116 (2020). https://doi.org/10.1109/access.2020.2968985
73. Zeng, Y., Zhang, Y.: Review of research on blockchain application development method. J. Phys. Conf. 1187(5), 52005 (2021). https://doi.org/10.1088/1742-6596/1187/5/052005
74. Zheng, X.: Research on blockchain smart contract technology based on resistance to quantum computing attacks. PLoS One 19(5), e0302325 (2024). https://doi.org/10.1371/journal.pone.0302325
75. Saha, R., et al.: A Blockchain framework in post quantum decentralization. J. Latex class files 11(4) (2012)
76. Naik, A. et al.: From portfolio optimization to Quantum blockchain and security: a systematic review of Quantum Computing in Finance. arxiv.org, papers 2307.01155, (2023)
77. Mahapatra, S., Wooldridge, T., Wang, X.: A post quantum blockchain application in M-band wavelet and Fresnel Domain: a Steganography based, decentralized, distributed ledger system. Trans. Eng. Comput. Sci. 3(1) (2022)
78. Buser, M., et al.: A survey on exotic signatures for post quantum blockchain: challenges and Research directions. Cryptology ePrint Archive 1 (2022). article 1
79. Kiktenko, E.O., et al.: Quantum-secured blockchain. Quantum Sci. Technol. 33(3), 35004 (2018). https://doi.org/10.1088/2058-9565/aabc6b
80. Bansod, S., Ragha, L.: Challenges in making blockchain privacy compliant for the digital world: some measures. Sādhanā 47(3), 168 (2022). https://doi.org/10.1007/s12046-022-01931-1
81. Abd El-Latif, A.A., et al.: Quantum-Inspired blockchain-based cybersecurity: securing smart edge utilities in IoT-based smart cities. Inf. Process. Manag. 58, 102549 (2021)
82. Sun, X., et al.: Towards quantum-secured permissioned blockchain: signature, consensus, and logic. Entropy 21(9), 887 (2019). https://doi.org/10.3390/e21090887
83. Rajan, D., Visser, M.: Quantum Blockchain using entanglement in time. Quan. Rep. 1(1), 3–11 (2019). https://doi.org/10.3390/quantum1010002
84. Li, J., et al.: Blockchain-based public auditing for big data in cloud storage. Inf. Process. Manag. 57(6), 102382 (2020). https://doi.org/10.1016/j.ipm.2020.102382
85. Abd-El-Atty, B., et al.: Optical image encryption based on quantum walks. Opt Laser. Eng. 138, 106403 (2021). https://doi.org/10.1016/j.optlaseng.2020.106403
86. Ahmed, A., et al.: Controlled alternate quantum walks based privacy preserving healthcare images in Internet of Things. Opt. Laser Technol. 124, 105942 (2020). https://doi.org/10.1016/j.optlastec.2019.105942
87. Habib, G., et al.: Blockchain technology: benefits, challenges, Applications and integration of Blockchain technology with cloud computing. Future Internet 14(11), 341 (2022). https://doi.org/10.3390/fi14110341
88. Gill, S.S. et al.: Quantum computing: vision and challenges, arxiv, (2024)
89. Horpenyuk, A., Opirskyy, I., Vorobets, P.: Analysis of problems and prospects of Implementation of post-quantum Cryptographic Algorithms. CEUR-WS Proc. 3504 (2023)
90. Abbasi, Q.H., et al.: Dive into the quantum realm: promise of quantum communication and what's next. IEEE CTN Issue (2024)
91. Rodenburg, B., Pappas, S.: Blockchain and Quantum Computing. MITRE Corporation (2017)

How to cite this article: S, M.G., et al.: Quantum blockchain: Trends, technologies, and future directions. IET Quant. Comm. 5(4), 516–542 (2024). https://doi.org/10.1049/qtc2.12119