2026 Volume: 02 Issue: 05 www.ijrpa.com ISSN 2456-9995 Research Article

International Journal Research Publication Analysis

Page: 01-32

A COMPREHENSIVE SURVEY ON POST–QUANTUM BLOCKCHAIN - BASED IDENTITY MANAGEMENT SYSTEMS.

*[1]Dr.Swathi K., [2]N Divish Kumar, [2]Prabhakara B. R., [2]Rohish C., [2]Rahul R Vasisht

[1]*Associate Professor, Jyothy Institute of Technology Bengaluru, India.*

[2]*Jyothy Institute of Technology Bengaluru, India.*

Article Received: 31 March 2026

Article Revised: 21 April 2026

Published on: 11 May 2026

***Corresponding Author: Dr. Swathi K.**

Associate Professor, Jyothy Institute of Technology Bengaluru, India.

DOI: https://doi-doi.org/101555/ijrpa.6267

ABSTRACT:

The rapid advancement of quantum computing introduces serious security challenges for existing blockchain and digital identity systems. Traditional cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC), which are widely used in authentication and blockchain systems, are vulnerable to quantum attacks through Shor's algorithm [2], [3]. At the same time, blockchain technology has enabled decentralized identity frameworks such as Self-Sovereign Identity (SSI), where users maintain ownership and control over their personal identity data without depending on centralized authorities [5], [11]. However, most blockchain identity systems still rely on classical cryptographic mechanisms and therefore remain vulnerable to future quantum threats. This survey paper presents a comprehensive study of Post-Quantum Blockchain-Based Identity Management Systems by integrating Post-Quantum Cryptography (PQC) with decentralized blockchain identity frameworks. The paper discusses the evolution from traditional centralized identity systems to blockchain-based decentralized identity and further toward quantum-resistant identity architectures. Important components such as decentralized identifiers (DIDs), verifiable credentials (VCs), smart contracts, zero-knowledge proofs (ZKPs), and quantum-resistant cryptographic algorithms including CRYSTALS-Kyber and CRYSTALS-Dilithium are examined. A comparative analysis of existing studies is presented to identify advantages, limitations, scalability issues, and security challenges. Finally, research gaps and future research directions are discussed for developing scalable, secure, privacy-preserving, and quantum-safe identity management systems

KEYWORDS**:** *Post-Quantum Cryptography, Blockchain Identity Management, Self-Sovereign Identity, Decentralized Identity, CRYSTALS-Kyber, CRYSTALS-*Di lithium*, Zero-Knowledge Proofs, Quantum Computing, Digital Identity Security, Smart Contracts.*

I. INTRODUCTION

Digital identity management has become an essential requirement in modern computing environments due to the increasing use of online services, cloud computing, banking applications, healthcare systems, and e-governance platforms. Traditional identity management systems are generally centralized in nature, where user information is stored and controlled by organizations or service providers. Although centralized systems provide ease of management, they suffer from several limitations including data breaches, identity theft, privacy issues, and lack of user control.

Blockchain technology introduced decentralized identity systems that allow users to manage and control their digital identities independently without relying on centralized authorities. This concept is referred to as Self-Sovereign Identity (SSI) [5], [11]. Blockchain-based identity systems use distributed ledgers and cryptographic verification mechanisms to provide transparency, integrity, decentralization, and tamper-resistant identity management. However, the security of current blockchain systems depends heavily on classical cryptographic algorithms such as RSA and ECC. These algorithms are based on mathematical problems such as integer factorization and discrete logarithms, which are computationally difficult for classical computers. However, quantum computers can efficiently solve these problems using Shor's algorithm, making existing cryptographic systems vulnerable [2], [3]. Post-Quantum Cryptography (PQC) addresses this issue by developing cryptographic algorithms that remain secure against both classical and quantum attacks. PQC algorithms are based on mathematical problems such as lattice-based cryptography, hash-based cryptography, code-based cryptography, and multivariate polynomial equations [3], [7]. The National Institute of Standards and Technology (NIST) has standardized quantum-resistant algorithms such as CRYSTALS-Kyber and CRYSTALS-Dilithium for secure communication and digital signatures [7].

The integration of PQC with blockchain-based identity

systems leads to the development of Post-Quantum Blockchain Identity Management Systems. These systems combine blockchain decentralization with quantum-resistant security to provide long-term protection for digital identities.

II. EVOLUTION OF SYSTEMS

2.1 Traditional Identity Systems

Traditional identity systems are based on centralized architectures where identity data is stored in centralized databases controlled by organizations. Examples include government ID systems, banking systems, and corporate authentication systems. While these systems provide centralized control and management, they suffer from several limitations:

- Single Point of Failure: If the central server is compromised, all identity data is at risk.
- Data Breaches: Large-scale breaches can expose sensitive personal information.
- Lack of User Control: Users do not have ownership of their identity data.
- Privacy Concerns: Organizations can misuse or share user data without consent.
- These limitations have led to the development of decentralized identity systems.

2.2 Blockchain-Based Identity Systems

Blockchain technology introduced a decentralized approach to identity management. Instead of storing identity data in a central server, blockchain distributes data across multiple nodes, ensuring transparency, immutability, and security.

Key features of blockchain-based identity systems include:

- Decentralization: No single authority controls identity data.
- Immutability: Data cannot be altered once recorded.
- Transparency: Transactions are verifiable.
- Security: Cryptographic techniques ensure data protection.

Self-Sovereign Identity (SSI) is a major application of blockchain in identity management. In SSI systems, users generate their own digital identities using cryptographic keys and share only necessary information with service providers [11].
However, these systems still rely on classical cryptography, which is not secure in a quantum computing environment.

2.3 Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography aims to develop cryptographic algorithms that remain secure even in the presence of quantum computers. PQC algorithms are based on

mathematical problems that are believed to be hard for both classical and quantum computers [3].

Key PQC approaches include:

- Lattice-Based Cryptography: Based on problems like Shortest Vector Problem (SVP) and Closest Vector Problem (CVP) [3].
- Hash-Based Cryptography: Uses hash functions for digital signatures.
- Code-Based Cryptography: Based on error-correcting codes.
- Multivariate Cryptography: Uses polynomial equations.
- NIST has standardized PQC algorithms such as:
- CRYSTALS-Kyber (Key Exchange)
- CRYSTALS-Dilithium (Digital Signatures)
- Falcon and SPHINCS+ (Alternative signature schemes) [7]

These algorithms provide strong security but introduce challenges such as increased key size and computational overhead.

2.4 Post-Quantum Blockchain Identity Systems

The integration of PQC with blockchain identity systems creates Post-Quantum Blockchain Identity Systems. These systems combine the benefits of blockchain such as decentralization and transparency with PQC-based quantum resistance.

Applications include:

- Secure digital identity for e-governance
- Quantum-safe financial transactions
- IoT device authentication
- Healthcare data management

III. SYSTEM COMPONENTS

A Post-Quantum Blockchain Identity System is composed of multiple interconnected modules that work together to provide secure, decentralized, and quantum-resistant identity management. Unlike traditional systems, this architecture integrates blockchain, cryptography, and privacy-preserving technologies to ensure robustness against future quantum threats.

3.1 Decentralized Identity Module

The decentralized identity module is responsible for creating and managing user identities using Decentralized Identifiers (DIDs). Unlike traditional identifiers such as usernames or email IDs, DIDs are globally unique and cryptographically verifiable.

Each user generates a DID along with a pair of cryptographic keys. The public key is stored on the blockchain, while the private key is securely stored by the user. This ensures that only the user has control over their identity.

Key features:

- Eliminates centralized identity providers
- Provides user ownership of identity
- Supports portability across platforms

This module forms the foundation of Self-Sovereign Identity (SSI) systems, where users are the sole controllers of their digital identity [11].

3.2 Post-Quantum Cryptographic Module

This module acts as the core security layer of the system. It replaces classical cryptographic algorithms with quantum-resistant algorithms such as:

- CRYSTALS-Dilithium (digital signatures)
- CRYSTALS-Kyber (key exchange)
- Falcon (efficient signatures) [7]

These algorithms are based on lattice problems that are computationally infeasible for both classical and quantum computers [3].

Key responsibilities include:

- Secure identity authentication
- Protection of communication channels
- Quantum-safe digital signatures

Challenges include:

- Larger key sizes
- Higher computational overhead
- Increased latency in transactions

Despite these challenges, PQC remains essential for future-proof security.

3.3 Blockchain Ledger Module

The blockchain ledger acts as a distributed database that stores identity-related information in a secure and immutable manner.

Instead of storing complete identity data, only hashed identity proofs and public keys are stored on-chain. This ensures privacy while maintaining verifiability.

Key properties include:

- Immutability (data cannot be altered)
- Transparency (verifiable by all nodes)
- Decentralization (no central authority) Popular blockchain platforms used include:
- Ethereum
- Hyperledger Indy
- Polygon

3.4 Authentication and Verification Module

This module verifies user identity using post-Quantum digital signatures. When a user attempts to access a service:

1. The user signs a challenge using their private key.
2. The system verifies it using the public key stored on blockchain.
3. If valid, access is granted. Advantages include:

- Password-less authentication
- Resistance to phishing attacks
- Strong cryptographic security

3.5 Zero-Knowledge Proof (ZKP) Module

Zero-Knowledge Proofs allow users to prove their identity without revealing actual personal information.

Example:

A user can prove they are above 18 years old without revealing their exact age [8].

Benefits include:

- Privacy preservation
- Selective disclosure

- Reduced data exposure

In Post-Quantum systems, integrating ZKP becomes more complex due to larger key sizes and increased computational requirements.

3.6 Smart Contract Module

Smart contracts automate identity verification and credential management processes.
Functions include:

Issuing identity credentials

- Verifying identity claims
- Controlling access permissions Advantages include:
- No intermediary requirement
- Transparent execution
- Reduced operational cost

3.7 Interoperability Module

This module enables identity systems to function across multiple blockchain platforms.
Example:

- An identity created on Ethereum can be used on Hyperledger.

This interoperability is essential for large-scale real-world adoption.

3.8 Storage Optimization Module

PQC introduces large cryptographic key sizes, increasing storage requirements.
To address this issue:

- Large data is stored off-chain using systems such as IPFS or cloud storage.
- Only hash references are stored on the blockchain. This improves:
- Scalability
- Speed
- Cost efficiency

IV. SYSTEM ARCHITECTURE

The Post-Quantum Blockchain Identity System follows a layered architecture that integrates decentralized identity, blockchain infrastructure, and Post-Quantum Cryptography. This architecture ensures secure, scalable, and privacy-preserving identity

management in a quantum computing environment.

The system is divided into multiple layers, each responsible for specific functionalities.

4.1 User Layer

The user layer represents end-users who create and manage their identities. Users generate decentralized identifiers (DIDs) and securely store their private keys. Identity ownership remains fully under user control, eliminating reliance on centralized authorities.

4.2 Identity Layer

This layer manages identity-related data such as:

- Decentralized Identifiers (DIDs)
- Verifiable Credentials (VCs)

Identity providers issue credentials that can be verified using cryptographic proofs. This layer ensures authenticity and integrity of identity data.

4.3 Blockchain Layer

The blockchain layer acts as a distributed ledger that stores identity proofs and public keys. It ensures:

- Immutability
- Transparency
- Decentralization

Instead of storing complete identity information, only hashed proofs are stored on-chain to maintain privacy.

4.4 Cryptographic Layer

This layer implements Post-Quantum Cryptographic algorithms such as:

- CRYSTALS-Kyber
- CRYSTALS-Di lithium
- Falcon [7]

These algorithms provide resistance against quantum attacks and secure all identity-related operations.

4.5 Application Layer

This layer includes real-world applications such as:

- Banking systems
- Healthcare systems
- E-governance platforms
- Cloud applications

These applications interact with the identity system for authentication and authorization purposes.

III. COMPARATIVE ANALYSIS OF EXISTING DATA

This section presents a comparative analysis of various research works related to Post-Quantum Cryptography and blockchain-based identity systems. The comparison is based on techniques, features, advantages, limitations, and application areas.

IV. *RESEARCH GAPS*

The literature survey reveals several important research gaps in existing Post-Quantum Blockchain Identity Systems..

- High computational complexity of PQC algorithms leading to increased processing time [2], [4].
- Scalability challenges in blockchain networks due to large cryptographic key sizes.
- Limited real-world deployment of Post-Quantum identity systems.
- Complexity in integrating Zero-Knowledge Proofs with PQC mechanisms [8].
- Inefficient key management and storage optimization techniques.
- Interoperability challenges between different blockchain platforms.
- Increased communication overhead in distributed systems.
- Limited lightweight solutions suitable for IoT and resource-constrained devices.

VI. FUTURE RESEARCH DIRECTIONS

Future research can focus on improving the scalability, efficiency, and usability of Post-Quantum Blockchain Identity Systems.

Important future research directions include:

- Development of lightweight Post-Quantum Cryptographic algorithms.
- Integration of Artificial Intelligence for intelligent identity verification.
- Hybrid cryptographic models combining classical cryptography with PQC.

- Improved blockchain scalability using Layer-2 solutions.
- Efficient storage optimization for large PQC keys.

Ref	Methods/ Algorithms	Advantages	Research Gap
[1]	Lattice-Based PQC	High efficiency	Hardware dependency
[2]	Kyber, Dilithium	Practical deployment	Integration complexity
[4]	PQ Digital Signatures Self-Sovereign	Strong security	High computation
[5]	dentity	Privacy preservation	Scalability issues
[6]	Hybrid PQC	Quantum-safe communication	Increased overhead
[7]	NIST PQC Standards	Trusted algorithms	Implementation issues
[8]	ZKP + PQC	Privacy-preserving verification	Complex integration
[9]	SSI + PQC	Secure decentralized identity	Performance trade-offs
[10]	Quantum Blockchain	Advanced security	Lack of practicality

VII. SECURITY ANALYSIS

Security is one of the most critical aspects of Post-Quantum Blockchain Identity Systems because these systems are designed to operate in environments where both classical and quantum attacks are possible.

Traditional cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC) are vulnerable to quantum attacks using Shor's algorithm [2], [3]. Post-Quantum Cryptographic algorithms such as CRYSTALS-Kyber and CRYSTALS-Dilithium are based on lattice problems that remain secure against both classical and quantum computers [7].

Another important aspect is privacy preservation. Zero-Knowledge Proofs (ZKPs) allow users to verify their identity without revealing sensitive information [8]. This reduces data exposure and improves confidentiality.

Major security advantages include:

- Resistance against quantum attacks
- Tamper-resistant identity storage
- Decentralized trust management
- Secure authentication mechanisms
- Privacy-preserving verification
- Reduced risk of identity theft

Thus, integrating blockchain technology with Post-Quantum Cryptography significantly improves the long-term security of digital identity systems.

VII. PERFORMANCE ANALYSIS

Performance is an important factor in evaluating the practicality of Post-Quantum Blockchain Identity Systems. Although these systems provide strong security, they also introduce several performance challenges.

One of the major issues is increased key size. Compared to classical cryptographic algorithms, PQC algorithms require significantly larger keys, resulting in higher storage and communication overhead [4].

Another challenge is computational complexity. PQC algorithms involve complex mathematical operations that increase encryption, decryption, and digital signature verification time [2].

Blockchain systems also face scalability limitations due to transaction throughput and storage constraints. Integrating PQC further increases blockchain storage requirements and transaction latency.

Major performance challenges include:

- Increased storage requirements
- Higher computational overhead
- Increased transaction processing time
- Communication overhead
- Scalability limitations

Despite these challenges, ongoing research is improving the efficiency and optimization of Post-Quantum Cryptographic algorithms for practical deployment.

XI. IMPLEMENTATION CHALLENGES

The implementation of Post-Quantum Blockchain-Based Identity Systems involves

several technical and operational challenges. Although these systems provide strong security and decentralization, practical deployment remains difficult due to computational, storage, and interoperability issues.

11.1 Computational Complexity

Post-Quantum Cryptographic algorithms require complex mathematical computations compared to classical cryptographic algorithms. Operations such as encryption, decryption, key generation, and digital signature verification consume more processing power and execution time [2], [4].

This computational overhead becomes a major concern in blockchain networks where multiple cryptographic operations are performed continuously.

11.2 Large Key Sizes

Most lattice-based PQC algorithms use significantly larger public and private keys compared to RSA and ECC. Larger key sizes increase:

- Storage requirements
- Network transmission overhead
- Blockchain transaction size
- Memory consumption

This directly impacts blockchain scalability and efficiency [6].

11.3 Scalability Issues

Blockchain systems already face scalability limitations due to transaction throughput and distributed ledger replication. Integrating PQC further increases storage and processing overhead.

Major scalability challenges include:

- Increased blockchain size
- Slow transaction validation
- High latency
- Increased consensus time

Layer-2 blockchain solutions and off-chain storage mechanisms can help reduce these scalability issues.

11.4 Interoperability Challenges

Different blockchain platforms use different protocols, consensus mechanisms, and

identity standards. This creates interoperability problems when identities need to function across multiple blockchain ecosystems.

For example:

- Ethereum uses smart contract-based identity systems.
- Hyperledger Indy uses decentralized identity frameworks.

Ensuring compatibility between these systems remains a major challenge.

11.5 Key Management Complexity

Securely storing and managing large PQC keys in decentralized environments is difficult. If users lose their private keys, identity recovery becomes challenging.

Important issues include:

- Secure key storage
- Backup and recovery mechanisms
- Multi-device synchronization
- Key revocation management

Efficient decentralized key management solutions are still under active research.

11.6 Energy Consumption

Post-Quantum Cryptographic operations require higher computational resources, which increases energy consumption in blockchain networks.

This becomes a major issue in:

- IoT environments
- Mobile devices
- Resource-constrained systems

Therefore, lightweight and energy-efficient PQC algorithms are required for practical deployment.

XII. APPLICATION OF POST-QUANTUM IDENTITY

Post-Quantum Blockchain Identity Systems can be applied across multiple domains where long-term security, privacy, and decentralized identity management are important.

12.1 E-Governance Systems

Governments can use decentralized quantum-safe identity systems for:

- Digital citizen identification
- Online voting systems

- Secure document verification
- Public service authentication

Blockchain ensures transparency and tamper-resistant record management, while PQC protects against future quantum attacks.

12.2 Healthcare Systems

Healthcare systems manage highly sensitive patient information that requires strong privacy and security protection.

Applications include:

- Secure patient identity management
- Medical record authentication
- Privacy-preserving data sharing
- Telemedicine authentication

Zero-Knowledge Proofs can help patients verify medical credentials without exposing sensitive information [8].

12.3 Banking and Financial Services

Financial institutions require secure authentication systems to prevent fraud and unauthorized access.

Applications include:

- Quantum-safe digital banking
- Secure financial transactions
- Fraud-resistant authentication
- Cross-border payment security

Blockchain decentralization combined with PQC improves transaction security and trust.

12.4 Internet of Things (IoT)

IoT devices require lightweight and secure identity mechanisms for device authentication.

Applications include:

- Smart home authentication
- Industrial IoT security
- Vehicle-to-vehicle communication
- Smart city infrastructure

However, implementing PQC in IoT remains challenging due to resource limitations [4].

12.5 Cloud Computing

Cloud platforms can use Post-Quantum Blockchain Identity Systems for:

- Secure cloud authentication
- Access control management
- Distributed identity verification
- Multi-cloud interoperability

Decentralized identity management improves trust and reduces dependence on centralized cloud providers.

12.6 Educational Platforms

Educational institutions can use blockchain-based identity systems for:

- Student credential verification
- Digital certificates
- Online examination authentication
- Academic record management

Quantum-resistant security ensures long-term protection of academic records.

XIII. ADVANTAGESOF POST-QUANTUM BLOCKCHAIN IDENTITY SYSTEMS

Post-Quantum Blockchain Identity Systems provide several advantages over traditional identity management systems.

13.1 Quantum Resistance

The major advantage is protection against quantum attacks. PQC algorithms remain secure even in the presence of powerful quantum computers [7].

13.2 Decentralization

Blockchain eliminates centralized authorities, reducing the risk of single points of failure and centralized attacks [5].

13.3 Improved Privacy

Zero-Knowledge Proofs and selective disclosure mechanisms improve user privacy by minimizing unnecessary data sharing [8].

User Ownership

Self-Sovereign Identity frameworks provide complete control of identity data to users rather than organizations [11].

13.4 Transparency and Immutability

Blockchain technology ensures that identity records are transparent, verifiable, and tamper-resistant.

13.5 Enhanced Security

The combination of blockchain and PQC provides multiple layers of security including:

- Secure authentication
- Tamper-resistant storage
- Distributed trust management
- Quantum-safe encryption

13.6 Reduced Identity Fraud

Cryptographic verification and decentralized validation significantly reduce identity theft and fraud.

13.7 Long-Term Data Protection

Quantum-resistant security ensures long-term protection for digital identities and sensitive information.

These advantages make Post-Quantum Blockchain Identity Systems highly suitable for future digital infrastructures and secure online ecosystems.

XIV. LIMITATIONS OF EXISTING SYSTEMS

Although Post-Quantum Blockchain Identity Systems provide strong security and decentralization, several limitations still exist in current implementations.

14.1 High Computational Overhead

Post-Quantum Cryptographic algorithms require complex mathematical computations, increasing processing time for encryption, decryption, and digital signature verification [2], [4]. This affects the overall efficiency of blockchain identity systems.

14.2 Increased Storage Requirements

Large cryptographic keys and signatures significantly increase blockchain storage requirements. Since blockchain data is replicated across multiple nodes, storage overhead becomes a major issue [6].

14.3 Network Latency

The integration of PQC algorithms can increase communication delays due to larger key transmission and verification processes. This leads to higher transaction latency in blockchain networks.

14.4 Scalability Problems

Blockchain systems already face scalability challenges related to transaction throughput and consensus mechanisms. PQC integration further increases computational and storage overhead, reducing scalability.

14.5 Complexity of Integration

Integrating blockchain technology, decentralized identity frameworks, and Post-Quantum Cryptography into a single architecture is highly complex.

Major integration challenges include:

- Compatibility between platforms
- Cryptographic standardization
- Identity interoperability
- Smart contract optimization

14.6 Lack of Standardized Frameworks

Although NIST has standardized several PQC algorithms [7], there is still no universal standard for implementing Post-Quantum Blockchain Identity Systems.

14.7 Limited Real-World Deployment

Most proposed systems remain at the research or prototype stage. Large-scale real-world deployment is still limited due to performance and infrastructure challenges.

XV. BLOCKCHAIN CONSENSUS MECHANISMS IN PQ IDENTITY SYSTEMS

Consensus mechanisms play an important role in maintaining trust, synchronization, and security within blockchain networks.

Different consensus algorithms can be used in Post-Quantum Blockchain Identity Systems depending on scalability and security requirements.

15.1 Proof of Work (PoW)

Proof of Work is one of the earliest blockchain consensus mechanisms used in Bitcoin.

Advantages:

- High security
- Decentralized validation Limitations:
- High energy consumption
- Slow transaction processing
- Poor scalability

Due to heavy computational requirements, PoW is less suitable for PQ identity systems.

15.2 Proof of Stake (PoS)

Proof of Stake selects validatorsbased on cryptocurrency ownership.

Advantages:

- Lower energy consumption
- Faster transaction processing
- Improved scalability

PoS-based blockchains are more suitable for integrating PQC mechanisms.

15.3 Practical Byzantine Fault Tolerance (PBFT) PBFT is commonly used in permissioned blockchain systems such as Hyperledger.

Advantages:

- Fast consensus
- Low latency
- High efficiency in private networks Limitations:
- Limited scalability in large distributed systems PBFT is useful for enterprise identity management systems.

15.4 Delegated Proof of Stake (DPoS)

DPoS uses elected validators to maintain blockchain consensus.

Advantages:

- High transaction throughput

- Reduced computational overhead Limitations:
- Partial centralization risk

DPoS can improve scalability in decentralized identity platforms.

15.5 Hybrid Consensus Models

Future Post-Quantum Blockchain Identity Systems may use hybrid consensus mechanisms combining:

- PoS
- PBFT
- Layer-2 scaling solutions

These approaches can improve scalability, efficiency, and security simultaneously.

XVI. ROLE OF SELF-SOVEREIGN IDENTITY (SSI)

Self-Sovereign Identity (SSI) is a decentralized identity model where users maintain complete ownership and control over their digital identities [11].

Unlike centralized identity systems, SSI eliminates dependence on third-party authorities for identity verification.

16.1 Working of SSI

In SSI systems:

1 Users create decentralized identifiers (DIDs).

2 Identity credentials are issued by trusted entities.

3 Credentials are stored securely by users.

4 Users selectively share credentials when required. Blockchain technology ensures secure and tamper-resistant credential verification.

4.1 Advantages of SSI

Important advantages include:

- User-controlled identity management
- Improved privacy
- Reduced dependence on centralized authorities
- Secure credential verification
- Better transparency and trust

4.2 SSI and Post-Quantum Security

Current SSI systems still rely on classical cryptographic algorithms. Integrating PQC into SSI frameworks is necessary for long-term security against quantum attacks.

Post-Quantum SSI systems can provide:

- Quantum-resistant authentication
- Secure credential sharing
- Privacy-preserving verification
- Long-term identity protection

4.3 Challenges in SSI Implementation

Major challenges include:

- Key management complexity
- Identity recovery mechanisms
- Interoperability issues
- Scalability limitations
- User adoption challenges

Despite these challenges, SSI remains one of the most promising approaches for decentralized digital identity management.

XVII. ROLE OF ZERO-KNOWLEDGE PROOFS (ZKP)

Zero-Knowledge Proofs are cryptographic techniques that allow users to prove information without revealing the actual data [8].

ZKPs are extremely important in privacy-preserving identity systems.

17.1 Working of ZKP

In a Zero-Knowledge Proof system:

- The prover demonstrates knowledge of information.
- The verifier confirms the proof without learning the actual data.

Example:

A user can prove they are above 18 years old without revealing their exact age.

17.2 Benefits of ZKP

Major advantages include:

- Privacy preservation
- Reduced data exposure
- Selective disclosure

- Improved confidentiality

17.3 ZKP in Blockchain Identity Systems

Blockchain identity systems use ZKPs for:

- Identity verification
- Credential authentication
- Privacy-preserving access control
- Secure data sharing

17.4 Challenges of ZKP Integration

Integrating ZKPs with PQC systems is challenging due to:

- Large proof sizes
- Increased computational complexity
- Verification overhead
- Scalability issues

Future research aims to develop lightweight and efficient Post-Quantum Zero-Knowledge Proof systems for decentralized identity management.

XVIII. ROLE OF SMART CONTRACTS IN IDENTITY MANAGEMENT

Smart contracts are self-executing programs stored on blockchain networks that automatically perform predefined operations when specific conditions are satisfied. In Post-Quantum Blockchain Identity Systems, smart contracts play an important role in automating identity verification, credential issuance, and access control management.

18.1Identity Credential Issuance

Smart contracts can automatically issue digital identity credentials after verifying required conditions.

Example:

- Educational institutions can issue blockchain-based academic certificates.
- Government organizations can issue decentralized digital identities.

These credentials remain immutable and verifiable on the blockchain.

18.2 Automated Verification

Smart contracts simplify identity verification processes by automatically validating user

credentials using cryptographic proofs.

Advantages include:

- Faster verification
- Reduced manual intervention
- Improved transparency
- Tamper-resistant authentication

18.3 Access Control Management

Smart contracts can control access permissions based on identity verification results.

Example:

- Healthcare systems can provide medical record access only to authorized doctors.
- Banking systems can restrict transaction access based on identity credentials.

This improves security and privacy protection.

18.4 Smart Contracts and PQC

Current smart contracts mainly rely on classical cryptographic mechanisms. Integrating Post-Quantum Cryptographic algorithms into smart contract systems is necessary for future quantum-resistant blockchain infrastructures.

However, this integration introduces challenges such as:

- Increased execution complexity
- Higher gas fees
- Smart contract optimization issues
- Increased transaction size

Research is ongoing to develop lightweight PQC-enabled smart contracts suitable for blockchain identity applications.

XIX. PRIVACY PRESERVATION IN POST-QUANTUM IDENTITY SYSTEMS

Privacy is one of the most important requirements in digital identity management systems. Traditional centralized identity systems often expose sensitive user information to service providers and third parties.

Post-Quantum Blockchain Identity Systems improve privacy through decentralization, cryptographic protection, and selective disclosure mechanisms.

19.1 Selective Disclosure

Selective disclosure allows users to share only the required identity information instead of exposing complete personal data.

Example:

- A user can verify citizenship without revealing full address details.
- A student can prove qualification without exposing complete academic history.

This reduces unnecessary data exposure.

19.2 Decentralized Data Control

In decentralized identity systems, users maintain ownership and control of their personal data [11].

Advantages include:

- Reduced dependence on centralized authorities
- Better user privacy
- Improved trust management
- Reduced data misuse

19.3 Zero-Knowledge Privacy Mechanisms

Zero-Knowledge Proofs improve privacy by enabling identity verification without revealing sensitive information [8].

Applications include:

- Age verification
- Financial authentication
- Healthcare identity verification
- Secure login systems

19.4 Blockchain Privacy Challenges

Although blockchain provides transparency, public blockchains may expose transaction metadata.

Privacy-related challenges include:

- Transaction traceability
- Metadata leakage
- Public visibility of blockchain records

To address these issues, advanced privacy-preserving mechanisms and encrypted identity storage solutions are required.

19.5 Future Privacy Enhancements

Future research may focus on:

- Advanced cryptographic privacy techniques
- Homomorphic encryption
- Secure multi-party computation
- Lightweight privacy-preserving protocols

These approaches can further strengthen privacy in Post-Quantum Blockchain Identity Systems.

XX. OVERALL ANALYSIS OF THE SURVEY

The literature survey clearly indicates that both blockchain technology and Post-Quantum Cryptography are rapidly evolving research domains with strong potential for securing future digital identity infrastructures.

Blockchain technology provides:

- Decentralization
- Transparency
- Tamper resistance
- User-controlled identity management

Self-Sovereign Identity frameworks further improve privacy and user ownership by eliminating centralized identity providers [11].

At the same time, Post-Quantum Cryptography provides resistance against future quantum attacks through algorithms based on lattice problems, hash functions, and other quantum-resistant mathematical foundations [3], [7].

However, both technologies individually face several limitations:

Limitations of Blockchain Identity Systems

- Lack of quantum resistance
- Scalability issues
- Storage overhead
- Privacy concerns

Limitations of PQC Systems

- Large key sizes
- Increased computational complexity
- Communication overhead
- Limited optimization for lightweight devices Therefore, integrating blockchain technology with Post-Quantum Cryptography becomes essential for developing future-proof identity systems.

The survey also reveals that:

- Most existing research focuses on either PQC or blockchain separately.
- Fully integrated Post-Quantum Blockchain Identity frameworks are still limited.
- Real-world deployment remains a major challenge.
- Efficient scalability and interoperability solutions are still under development.

Despite these challenges, Post-Quantum Blockchain Identity Systems provide a highly promising solution for future digital ecosystems where long-term security, privacy preservation, decentralization, and quantum resistance are essential.

Future advancements in:

- Lightweight PQC algorithms
- Layer-2 blockchain solutions
- Privacy-preserving protocols
- Cross-chain interoperability
- AI-assisted identity verification

can significantly improve the practicality and scalability of these systems.

Thus, Post-Quantum Blockchain-Based Identity Management Systems represent an important step toward building secure, decentralized, and future-ready digital identity infrastructures for the quantum computing era.

XXI. COMPARISON BETWEEN TRADITIONAL, BLOCKCHAIN, AND POST-QUANTUM IDENTITY SYSTEMS

Identity management systems have evolved from traditional centralized models to decentralized blockchain-based frameworks and finally toward Post-Quantum secure identity architectures. Traditional identity systems depend on centralized databases

managed by organizations or service providers. These systems are commonly used in banking, healthcare, education, and government services. Although centralized systems are easy to manage, they suffer from major limitations such as single points of failure, data breaches, identity theft, lack of transparency, and limited user control. In addition, traditional systems rely heavily on classical cryptographic algorithms such as RSA and ECC, which are vulnerable to quantum attacks [2], [3].

Blockchain-based identity systems introduced decentralization into identity management. Instead of relying on centralized authorities, blockchain distributes identity verification across multiple nodes [5]. Self-Sovereign Identity (SSI) frameworks further improve identity management by allowing users to control and manage their own credentials securely [11]. Blockchain identity systems provide transparency, immutability, and tamper-resistant storage, which significantly improve trust and security. However, these systems still depend on classical cryptographic algorithms and therefore remain vulnerable to future quantum computing attacks.

Post-Quantum Blockchain Identity Systems combine blockchain decentralization with quantum-resistant cryptographic algorithms to provide future-proof security. These systems use PQC algorithms such as CRYSTALS-Kyber and CRYSTALS-Dilithium to secure authentication and communication processes [7]. In addition to decentralization and transparency, these systems provide resistance against quantum attacks and improved privacy preservation. Although Post-Quantum systems offer strong security advantages, they still face challenges related to computational overhead, scalability, storage requirements, and implementation complexity.

The comparison between these systems clearly shows that Post-Quantum Blockchain Identity Systems provide a more secure and future-ready solution for digital identity management by combining decentralization, privacy preservation, transparency, and quantum-resistant security.

XXII. INDUSTRIAL AND REAL-WORLD ADOPTION

The adoption of Post-Quantum Blockchain Identity Systems is gradually increasing across multiple industries due to growing concerns regarding cybersecurity, privacy protection, and future quantum threats. Financial institutions require highly secure authentication systems to protect sensitive customer information and financial transactions. Blockchain-based identity systems combined with Post-Quantum Cryptography can provide secure digital banking, fraud-resistant authentication, and

quantum-safe transaction verification.

Healthcare systems also require strong privacy-preserving identity management solutions because they handle confidential patient information. Post-Quantum Blockchain Identity Systems can improve patient authentication, electronic health record management, telemedicine security, and secure medical data sharing. Zero-Knowledge Proofs further improve healthcare privacy by allowing patients to verify information without revealing sensitive data [8].

Governments and e-governance platforms are increasingly exploring blockchain-based identity frameworks for digital citizen identification, online voting systems, and secure public service authentication. Since government records require long-term security protection, integrating quantum-resistant cryptographic algorithms becomes highly important.

Educational institutions can use blockchain identity systems for digital certificates, academic transcript verification, and secure student authentication. These systems reduce certificate forgery and improve verification efficiency. Similarly, telecom and cloud service providers can use decentralized Post-Quantum identity systems for secure access management, subscriber authentication, and distributed resource sharing [9].

Despite these advantages, industrial adoption still faces challenges such as implementation cost, scalability limitations, lack of standardization, and integration complexity. Many existing systems remain at the prototype stage, and large-scale real-world deployment is still limited. However, ongoing research in blockchain scalability, lightweight PQC algorithms, artificial intelligence, and decentralized identity frameworks is expected to improve the practicality of Post-Quantum Blockchain Identity Systems in the future.

As quantum computing technology continues to evolve, organizations are expected to increasingly adopt quantum-resistant blockchain identity frameworks to secure next-generation digital infrastructures.

XXIII. DISCUSSION

The rapid growth of digital technologies has significantly increased the importance of secure identity management systems. Traditional centralized identity architectures are no longer sufficient to handle modern cybersecurity threats because they suffer from data breaches, identity theft, and privacy violations. Blockchain technology addressed many of these problems by introducing decentralization, transparency, and tamper-resistant

identity management mechanisms. However, the emergence of quantum computing introduces a new security challenge that can potentially break classical cryptographic algorithms used in existing blockchain systems.

Post-Quantum Cryptography has emerged as a promising solution for protecting digital infrastructures against quantum attacks. Algorithms such as CRYSTALS-Kyber and CRYSTALS-Dilithium provide strong resistance against quantum adversaries while maintaining cryptographic security [7]. Integrating these algorithms with blockchain-based identity systems creates a more secure and future-ready digital identity framework.

The survey also highlights that Self-Sovereign Identity frameworks are becoming increasingly important because they provide users with ownership and control over their identity data [11]. This reduces dependence on centralized authorities and improves privacy preservation. Additionally, technologies such as Zero-Knowledge Proofs further strengthen privacy by enabling selective disclosure and confidential verification [8].

Despite these advantages, several practical challenges remain unresolved. PQC algorithms introduce larger key sizes and higher computational complexity, which affect blockchain scalability and transaction performance. Interoperability between different blockchain platforms is another major challenge because different systems follow different identity standards and consensus mechanisms.

The survey indicates that future research should focus on developing lightweight and scalable Post-Quantum identity solutions suitable for real-world applications. Improvements in blockchain scalability, storage optimization, and efficient cryptographic implementations are necessary for practical deployment. Artificial Intelligence and machine learning techniques may also help improve identity verification and fraud detection in decentralized systems.

Overall, Post-Quantum Blockchain Identity Systems represent a significant advancement toward secure and decentralized digital identity management for the quantum computing era.

XXIV. FINAL OBSERVATION

From the overall study, it is observed that the integration of blockchain technology and Post-Quantum Cryptography provides a strong foundation for future digital identity systems. Traditional centralized systems are increasingly becoming vulnerable to cyberattacks and privacy issues, while blockchain-based systems alone cannot fully resist future quantum threats.

Post-Quantum Blockchain Identity Systems overcome these limitations by combining decentralization, transparency, privacy preservation, and quantum-resistant security into a unified framework. Technologies such as Self-Sovereign Identity, Decentralized Identifiers, Zero-Knowledge Proofs, and smart contracts further improve trust, authentication, and identity ownership.

Although several challenges related to scalability, storage overhead, interoperability, and computational complexity still exist, ongoing advancements in Post-Quantum Cryptography and blockchain research are continuously improving the efficiency and practicality of these systems. Therefore, Post-Quantum Blockchain Identity Systems are expected to play an important role in securing future digital ecosystems including banking, healthcare, cloud computing, IoT, e-governance, and distributed communication networks. These systems provide a promising pathway toward secure, decentralized, privacy-preserving, and future-ready identity management infrastructures.

XXV. CONCLUSION

This survey paper presented a detailed study of Post-Quantum Blockchain-Based Identity Management Systems and emphasized the importance of developing secure and future-ready digital identity frameworks in the quantum computing era. Traditional identity management systems rely heavily on centralized architectures and classical cryptographic algorithms such as RSA and ECC, which are vulnerable to future quantum attacks [2], [3]. Although blockchain technology improved identity management by introducing decentralization, transparency, and Self-Sovereign Identity frameworks, most existing blockchain identity systems still depend on classical cryptographic mechanisms and therefore remain vulnerable to quantum computing threats [5], [11].

The survey examined the evolution of identity management systems from traditional centralized models to blockchain-based decentralized architectures and finally toward Post-Quantum secure identity frameworks. Important technologies such as decentralized identifiers, verifiable credentials, smart contracts, blockchain ledgers, Zero-Knowledge Proofs, and Post-Quantum Cryptographic algorithms including CRYSTALS-Kyber and CRYSTALS-Dilithium were analyzed in detail [7], [8]. The integration of these technologies provides strong authentication, privacy preservation, tamper-resistant storage, and decentralized trust management.

The comparative analysis revealed that most existing research works focus either on blockchain identity management or Post-Quantum Cryptography independently. Only

limited research attempts to integrate both technologies effectively into a single scalable framework. Existing systems still face several challenges such as computational overhead, large cryptographic key sizes, interoperability issues, storage complexity, scalability limitations, and lack of real-world deployment. These challenges indicate that significant research and optimization are still required before large-scale industrial adoption becomes practical.

The survey also highlighted the growing importance of Self-Sovereign Identity systems in modern digital ecosystems. SSI frameworks improve user privacy and control by eliminating dependence on centralized identity providers [11]. Similarly, Zero-Knowledge Proofs enhance confidentiality by allowing selective disclosure and secure identity verification without revealing sensitive information [8]. These technologies play an important role in building privacy-preserving and user-centric digital identity systems.

Furthermore, the study demonstrated that Post-Quantum Blockchain Identity Systems have wide-ranging applications across multiple domains including banking, healthcare, e-governance, cloud computing, IoT, telecommunications, and education. As digital infrastructures continue to expand globally, the need for secure and quantum-resistant identity management systems will become increasingly critical.

Although several technical and implementation challenges remain unresolved, ongoing advancements in Post-Quantum Cryptography, blockchain scalability, distributed identity frameworks, and artificial intelligence are continuously improving the feasibility of these systems. Future research focusing on lightweight PQC algorithms, efficient blockchain architectures, cross-chain interoperability, and advanced privacy-preserving mechanisms can significantly improve performance and usability.

In conclusion, Post-Quantum Blockchain-Based Identity Management Systems represent a promising solution for securing future digital identities against both classical and quantum threats. By combining blockchain decentralization with quantum-resistant cryptographic security, these systems provide a strong foundation for building secure, transparent, privacy-preserving, and future-ready digital identity infrastructures for the next generation of computing environments.

In addition, the adoption of Post-Quantum Blockchain Identity Systems can significantly improve trust and reliability in digital ecosystems by reducing dependence on centralized authorities and minimizing the risks associated with identity theft, data breaches, and unauthorized access. As organizations increasingly shift toward cloud-based and decentralized infrastructures, secure digital identity management becomes a fundamental

requirement for maintaining cybersecurity and user privacy. The integration of blockchain technology with Post-Quantum Cryptography provides a long-term security solution capable of protecting sensitive information even in the presence of advanced quantum computing technologies. This makes Post-Quantum identity frameworks highly suitable for critical sectors such as national security, defense systems, financial institutions,healthcare infrastructures, and global communication networks.

Moreover, the continuous evolution of emerging technologies such as Artificial Intelligence, Internet of Things (IoT), edge computing, and distributed cloud systems will further increase the demand for scalable and secure decentralized identity solutions. Future digital environments will require identity systems that are not only secure and privacy-preserving but also highly interoperable, efficient, and user-friendly. Therefore, the development of standardized and optimized Post-Quantum Blockchain Identity frameworks will play an important role in shaping the next generation of secure digital infrastructures. With continued research, industrial collaboration, and technological advancements, Post-Quantum Blockchain-Based Identity Management Systems are expected to become a core component of future cybersecurity architectures and decentralized digital ecosystems.

REFERENCE

1 J. Howe and B. Westerbaan, “Benchmarking and Analysing the NIST PQC Lattice-Based Signature Schemes Standards on the ARM Cortex M7,” in *Proceedings of Post-Quantum Cryptography Research*, 2022.

2 E. D. Demir, B. Bilgin, and M. C. Onbasli, “Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms,” *arXiv preprint arXiv:2503.12952*, 2025.

3 C. Zong, “Some Mathematical Problems Behind Lattice-Based Cryptography,” *arXiv preprint arXiv:2506.23438*, 2025.

4 M. Vidaković and K. Miličević, “Performance and Applicability of Post-Quantum Digital Signature Algorithms in Resource-Constrained Environments,” *Algorithms*, vol. 16, no. 518, pp. 1–18, 2023.

5 Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. R. Choo, “Blockchain-Based Identity Management Systems: A Review,” *Journal of Network and Computer Applications*, 2020.

6 P. Nwaga and S. Idima, “Post-Quantum Cryptographic Algorithms for Secure

Communication in Decentralized Blockchain and Cloud Infrastructure," *International Journal of Computer Applications Technology and Research*, vol. 11, no. 4, pp. 155–170, 2022.

7 G. Alagic et al., "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process," *NIST Interagency Report 8413*, National Institute of Standards and Technology, 2022.

8 S. Dutto, D. Margaria, C. Sanna, and A. Vesco, "Toward a Post-Quantum Zero-Knowledge Verifiable Credential System for Self-Sovereign Identity," in *Proceedings of Cryptography and Security Research*, 2023.

9 E. Zeydan, L. Blanco, J. Mangues-Bafalluy, S. S. Arslan, and Y. Turk, "Post-Quantum Blockchain-Based Decentralized Identity Management for Resource Sharing in Open Radio Access Networks," *IEEE Conference on Cloud Networking*, 2021.

10 Z.-Z. Sun, Y.-B. Cheng, M. Wang, L. Qian, D. Ruan, and G.-L. Long, "Quantum Blockchain Relying on Quantum Secure Direct Communication Network," *IEEE Access*, 2021.

11 M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," *IEEE Access*, vol. 7, pp. 103059–103079, 2019.

12 K. Samunnisa and S. V. K. Gaddam, "Blockchain-Based Decentralized Identity Management for Secure Digital Transactions," *Synthesis: A Multidisciplinary Research Journal*, vol. 1, no. 2, pp. 22–29, 2023.

13 B. Zohuri, H. T. Nguyen, and M. Moghaddam, "What is Cryptocurrency? Is it a Threat to Our National Security, Domestically and Globally?" *International Journal of Theoretical & Computational Physics*, vol. 3, no. 1, pp. 1–14, 2022.