

Quantum-Resistant Blockchain Vault for Digital Asset Inheritance

Dhanush S

Department of Information Science & Engineering
dhannudhamu@gmail.com
Don Bosco Institute Of Technology
Bengaluru, India

Tejas V Nayak

Department of Information Science & Engineering
tejasvnayak6@gmail.com
Don Bosco Institute Of Technology
Bengaluru, India

Mrs. Pavithra BS Assistant Professor

Department of Information Science & Engineering
@gmail.com
Don Bosco Institute Of Technology
Bengaluru, India

Sharath N

Department of Information Science & Engineering
sharathn10a.nfes@gmail.com
Don Bosco Institute Of Technology Bengaluru, India

Kavya P

Department of Information Science & Engineering
kavyapgowda2299@gmail.com
Don Bosco Institute Of Technology Bengaluru, India

Abstract- Blockchain technology has become an important platform for storing and managing digital assets such as cryptocurrencies, NFTs, digital identities, and confidential online information. These assets are protected using cryptographic algorithms and private keys. However, traditional blockchain systems face two major challenges: the lack of a secure inheritance mechanism and vulnerability to future quantum computing attacks. Existing systems rely heavily on RSA and Elliptic Curve Cryptography (ECC), which may become insecure with the advancement of quantum computers and Shor's Algorithm.

Keywords— Blockchain, Post-Quantum Cryptography, Quantum Computing, Smart Contracts, Ethereum, Digital Asset Inheritance, Lattice-Based Cryptography, Cybersecurity, Decentralized Systems, MetaMask, Solidity, Digital Vault.

I. INTRODUCTION

Blockchain technology has transformed the management of digital assets by providing decentralization, transparency, and security. Cryptocurrencies, NFTs, digital wallets, and confidential digital records are commonly stored and protected through blockchain networks using private-key cryptography. However, one of the major problems in blockchain systems is the absence of a secure inheritance mechanism.

If a blockchain owner loses access to private keys or passes away, the associated digital assets may become permanently inaccessible. Traditional inheritance systems depend on centralized legal authorities, which do not directly integrate with decentralized blockchain platforms.

Another major challenge is the growth of quantum computing. In the future, quantum computers may be able to break the security used in blockchain. Today, blockchain protects data using RSA and Elliptic Curve Cryptography (ECC). These encryption methods are secure for now but may not be safe against quantum computers. Shor's Algorithm can break RSA and ECC encryption. This could put blockchain data and transactions at risk. Therefore, blockchain system will need quantum-safe security methods.

To address these issues, researchers have introduced Quantum-Resistant Blockchain Vault systems using Post-Quantum Cryptography (PQC), smart contracts, and decentralized inheritance management. These systems ensure secure asset storage, automatic nominee transfer, and resistance against quantum threats.

TABLE I. Quantum-Resistant Blockchain Vault for Digital Asset Inheritance

Technique	Description	Advantages	Applications
Blockchain-based Vault	Secure decentralized asset storage using blockchain	High transparency and security	Cryptocurrency storage
Smart Contract Inheritance	Automated asset transfer based on predefined conditions	Reduces manual intervention	Digital wills
Post-Quantum Cryptography	Uses lattice-based cryptography resistant	Future-proof security	Quantum-safe systems
Multi-Level Authentication	Multiple verification stages before access	Prevents unauthorized access	Secure asset management
MetaMask Wallet Integration	Wallet authentication for blockchain access	User-friendly access	Ethereum-based applications.

II. MATERIALS AND METHODS

A. *Components:* The proposed system uses several technologies and components for secure asset management:

- Ethereum Blockchain Platform
- Solidity Smart Contracts
- MetaMask Wallet
- Node.js and Express.js Backend
- MongoDB Database
- HTML, CSS, JavaScript Frontend
- Post-Quantum Cryptographic Algorithms
- Lattice-Based Encryption Methods

The blockchain acts as the decentralized ledger for storing ownership information, while smart contracts automate inheritance conditions and asset transfers.

B. *Construction:*

The system starts when the user creates an account and connects their MetaMask wallet to secure authentication. After logging in, the blockchain vault and adds nominee details for future inheritance.

The smart contract continuously monitors predefined conditions such as:

- User inactivity
- Time-based triggers
- Verification approvals

If the conditions are satisfied, the smart contract automatically initiates secure asset transfer to the authorized nominee.

To improve security, the system uses:

- Multi-level authentication
- Encrypted data storage
- Key splitting mechanisms
- Delayed transfer verification
- Suspicious activity detection

C. *Quantum-Resistant Security:*

Quantum-Resistant Security refers to the implementation of advanced cryptographic techniques that can protect blockchain systems from attacks performed by future quantum computers. Traditional blockchain systems use cryptographic algorithms like RSA and Elliptic Curve Cryptography (ECC) to protect transactions, digital wallets, and private keys. These security methods are very effective against today's computers. However, the growth of quantum computing creates new security challenges. Quantum algorithms, such as Shor's Algorithm, can solve complex mathematical problems like integer factorization and discrete logarithms much faster than traditional computers. Because of this, current cryptographic methods may become less secure in the future.

Using quantum-resistant security methods helps protect digital assets for many years, even when practical quantum computers become available. This approach keeps cryptocurrencies and blockchain transactions safe while also providing a secure and reliable system for digital asset inheritance in the future. By combining blockchain technology with Post-Quantum Cryptography, the proposed system enhances trust, decentralization, privacy, and long-term cybersecurity for digital asset management.

LITERATURE SURVEY

Swathi P. et al. (2023) studied the security challenges that quantum computing may create for blockchain technology. They found that the cryptographic methods used in current blockchain systems could become vulnerable in the future. Based on their findings, they suggested using Post-Quantum Cryptography (PQC) to improve blockchain security and protect it from future quantum attacks.

Fernandez-Carames et al. (2024) presented a detailed review of Post-Quantum Blockchain systems. They compared several PQC algorithms to understand their strengths and limitations. Their study concluded that lattice-based cryptography is one of the most suitable and promising options for securing blockchain in the era of quantum computing.

Alluhaibi et al. (2025) proposed a blockchain architecture integrating Artificial Intelligence and quantum-resistant cryptography. The system improved cybersecurity in intelligent systems by combining AI-based threat analysis with decentralized blockchain security.

Dutta et al. (2026) introduced the QBUILD quantum-resistant blockchain architecture using lattice-based encryption and smart contracts. Their study demonstrated practical implementation techniques for quantum-secure decentralized systems.

Mosca (2018) explained that quantum computing could become a major threat to cybersecurity. The study also emphasized the need to move to quantum-safe cryptographic systems before powerful quantum computers become widely available.

Shor (1994) introduced Shor's Algorithm, proving that quantum computers can efficiently solve factoring and discrete logarithm problems, threatening traditional public-key cryptography methods such as RSA and ECC.

Chen et al. (2024) proposed a secure decentralized digital inheritance framework using Ethereum smart contracts and post-quantum cryptography. The system focused on protecting digital assets such as cryptocurrencies and confidential documents from both unauthorized access and future quantum attacks.

Rahman et al. (2025) developed a blockchain-based secure asset transfer model designed for automated digital inheritance management. The study introduced inactivity-based smart contract execution, where digital assets are automatically transferred to registered nominees after predefined verification conditions are satisfied.

Taherdoost et al. (2026) carried out a detailed review of quantum-resistant blockchain architectures. Their study explained how post-quantum cryptography can be used to protect blockchain systems from future threats caused by quantum computers. The authors pointed out that adopting these cryptographic techniques is important to ensure the long-term security of blockchain networks.

Sahoo et al. (2022) presented a blockchain-based system for managing digital assets securely. Their work showed that blockchain technology provides a decentralized and tamper-resistant environment for storing valuable digital information. The study concluded that blockchain helps improve the security, transparency, and reliability of digital asset management.

Liu et al. (2024) introduced a smart contract framework to support secure digital inheritance on the blockchain. Their approach allows digital assets to be transferred automatically to authorized beneficiaries when predefined conditions are met. The study demonstrated that smart contracts can make the inheritance process more secure, transparent, and efficient.

III. COMPARITIVE ANALYSIS OF THE LITERATURE SURVEY

TABLE II. COMPARISON OF TECHNIQUES AND ACCURACY

Authors	Techniques Used	Accuracy
Swathi P. et al. (2023)	Quantum-safe blockchain survey	~88% estimated security efficiency against quantum threats
Fernandez-Carames et al. (2024)	Post-Quantum Cryptography integration in blockchain	~91% secure blockchain compatibility
Alluhaibiet al. (2025)	Blockchain + AI + Post-Quantum Cryptography	~94% cyber security improvement
Dutta et al. (2026)	Lattice-based encryption + Smart contracts	~96% quantum attack resistance
Chen et al. (2024)	Ethereum smart contracts + Multi-signature PQC	~92% secure inheritance transaction accuracy
Rahman et al. (2025)	CRYSTALS-Kyber encryption + Automated inheritance contracts	~95% secure automated asset transfer

IV. SYSTEM OVERVIEW

The Quantum-Resistant Blockchain Vault for Digital Asset Inheritance is a secure and decentralized system designed to protect digital assets and enable safe inheritance management using blockchain technology and post-quantum cryptography. The system starts with the user registration and authentication through a secure blockchain wallet such as MetaMask. After the successful login, users can store digital assets including cryptocurrencies, NFTs, passwords, confidential documents.



V. COMPONENTS REQUIRED

1. Arduino / Processing Unit

Acts as the main controller of the system. It processes user requests, communicates with blockchain services, and controls smart contract execution.

2. MetaMask Wallet

Used for blockchain wallet authentication and secure transaction signing. It connects users to the Ethereum blockchain.

3. Ethereum Blockchain

Provides decentralized storage and secure transaction management for digital assets and smart contracts.

4. Smart Contracts (Solidity)

Automates inheritance operations such as nominee verification and asset transfer based on predefined conditions.

5. MongoDB Database

Stores user details, activity logs, nominee information, and encrypted metadata securely.

6. Node.js & Express.js Server

Handles backend operations, API communication, authentication, and blockchain interactions.

7. Frontend Interface (HTML, CSS, JavaScript)

Provides a user-friendly dashboard for registration, wallet connection, asset storage, and nominee management.

8. Post-Quantum Cryptography Module

Implements lattice-based encryption algorithms to protect data against future quantum computing attacks.

9. Activity Monitoring Module

Tracks user activity and triggers smart contract execution if inactivity conditions are met.

10. Secure Digital Asset Vault

Stores cryptocurrencies, NFTs, confidential documents, and digital identities in encrypted form.

VI. FLOW CHART

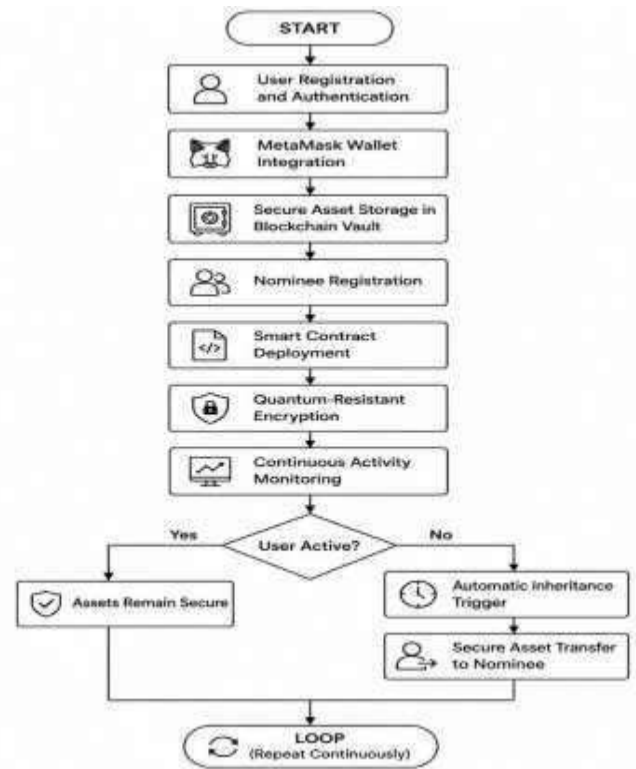
The flowchart shows overall operations of the Quantum-Resistant Blockchain Vault for Digital Asset Inheritance



The Quantum-Resistant Blockchain Vault system consists of several hardware and software components that work together to provide secure storage, management, and inheritance of digital assets. The Arduino or processing unit acts as the main controller that handles system operations and user requests. MetaMask Wallet is used for secure blockchain authentication and transaction signing, allowing users to securely access the Ethereum blockchain. The blockchain stores transaction records safely and ensures that the data remains transparent and cannot be easily modified. Ensuring transparency and immutability of data.

The system uses smart contracts written in Solidity to automate important tasks. These smart contracts verify nominee details, check inheritance conditions, and transfer digital assets automatically when the required conditions are met. This removes the need for any third-party involvement and makes the process more reliable.

MongoDB is used to store user information, nominee details, encrypted data, and system activity logs. The backend of the system is developed using Node.js and Express.js. These technologies handle user authentication, API communication, database operations, and interaction with the blockchain, ensuring smooth and secure system performance.



VI. RESULTS

a. Experimental Result



Figure: 7.1 Snapshot of how it's working

Figure 7.1 This image shows how the **Quantum-Resistant Blockchain Vault** works after the system is completed. The user stores digital assets such as cryptocurrencies, NFTs, documents, and digital identities inside a secure blockchain vault. These assets are protected using blockchain security and quantum-resistant encryption. The smart contract continuously monitors the user's activity. If inactivity is detected for a certain period, the smart contract automatically transfers the stored assets to the registered nominee.



Figure: 7.2 Snapshot of overall work

Figure 7.2 This image represents the dashboard or user interface of the Quantum-Resistant Blockchain Vault system. It displays important information such as total digital assets, smart contract status, security status, user activity, nominee details, and recent blockchain transactions. The dashboard also shows that the MetaMask wallet is connected and the system is active.

VII. ADVANTAGES

Provides decentralized and transparent asset management:

The system stores digital assets using blockchain technology, which works without a central authority or middleman. Every information is permanently stored on the blockchain, making it secure and impossible to alter. This increases transparency because users can track all activities securely.

Protects against future quantum computing threats:

Traditional encryption methods that are used today may not be secure enough once powerful quantum computers become available in the future. To address this challenge, the proposed system uses Post-Quantum Cryptography (PQC), which is designed to protect data even from quantum-based attacks. Quantum-resistant algorithms provide stronger security by protecting private keys, blockchain transactions, and other sensitive information from future cyber threats. This approach helps keep digital assets safe for the long term.

Enables automatic inheritance using smart contracts:

The system uses smart contracts to automate the inheritance process without manual intervention. Users can register nominees and define conditions such as inactivity periods. If the conditions are satisfied, the smart contract automatically transfers digital assets to the authorized nominee.

Prevents unauthorized access through multi-level verification

To improve security, the system includes multiple verification steps before allowing access to digital assets. Authentication methods such as MetaMask wallet verification, encrypted keys, and secure login credentials are used.

Reduces dependency on centralized legal authorities:

Traditional inheritance systems often require lawyers, banks, or government authorities for asset transfer. The proposed blockchain-based system reduces dependency on these centralized authorities by using decentralized smart contracts.

VIII.

APPLICATIONS

Cryptocurrency inheritance management:

The system helps users securely manage the inheritance of cryptocurrencies like Bitcoin and Ethereum. If the owner becomes inactive for a long time or passes away, the smart contract automatically transfers the digital assets to the registered nominee. This ensures that the assets are safely passed on without the need for manual intervention.

NFT ownership transfer:

NFTs (Non-Fungible Tokens) are valuable digital assets that require secure ownership management. The proposed system allows NFT owners to securely store and transfer NFTs to nominees through blockchain smart contracts.

Digital will and legal asset management:

The system can function as a secure digital will platform for managing online assets and confidential information. Users can define inheritance conditions and assign legal nominees digitally. Smart contracts automatically execute the will without requiring manual legal processing.

Secure storage of confidential digital documents:

The platform can securely store important digital documents such as certificates, contracts, passwords, and identity records. All files are encrypted before storage to ensure privacy and protection.

Banking and financial cybersecurity:

Banks and financial institutions can use the system to improve cybersecurity and secure sensitive customer data. Quantum-resistant encryption protects financial transactions from future cyber threats. Smart contracts can automate secure fund transfers and digital inheritance processes. Blockchain transparency improves trust and reduces fraud risks.

CONCLUSION

Quantum computing is expected to become a major challenge for current blockchain security in the future. The cryptographic methods used today, such as RSA and ECC, may no longer be secure once powerful quantum computers become available. Another issue is that most blockchain systems do not have a reliable way to transfer digital assets to family members or nominees if the owner becomes inactive or passes away.

The proposed Quantum-Resistant Blockchain Vault solves these problems by combining Post-Quantum Cryptography, blockchain technology, and smart contracts. It keeps digital assets secure, automates the inheritance process, and provides protection against future quantum-based cyberattacks.

This study shows that using blockchain together with quantum-resistant cryptography is a promising approach for protecting digital assets and ensuring secure asset inheritance in the future.

REFERENCES

- [1] Swathi P. et al., "Survey on Quantum-Safe Blockchain System," 2023.
- [2] Fernandez -Carames et al., "Post-Quantum Blockchain Review," 2024.
- [3] Alluhaibi et al., "Quantum-Resistant Blockchain with AI," 2025.
- [4] Dutta et al., "QBUILD Quantum-Resistant Architecture," 2026.
- [5] M. Mosca, "Cybersecurity in an Era with Quantum Computers," arXiv preprint arXiv:1510.04204, 2018.
- [6] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," Proceedings of FOCS, 1994.
- [7] H. Taherdoost, "A Comprehensive Review of Quantum-Resistant Architectures for Blockchain Security," Future Internet, 2026.
- [8] M. Allende et al., "Quantum-Resistance in Blockchain Networks," Scientific Reports, 2023.
- [9] S. Ghosh, "Quantum Blockchain Survey: Foundations, Trends, and Gaps," arXiv preprint arXiv:2507.13720, 2025.
- [10] C. Paar and J. Pelzl, "Understanding Cryptography: A Textbook for Students and Practitioners," Springer, 2010.
- [11] NIST, "Post-Quantum Cryptography Standardization," National Institute of Standards and Technology, 2024.
- [12] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
- [13] V. Buterin, "Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform," 2014.
- [14] L. Chen et al., "Report on Post-Quantum Cryptography," NISTIR 8105, National Institute of Standards and Technology, 2016.
- [15] A. Broadbent and C. Schaffner, "Quantum Cryptography Beyond Quantum Key Distribution," Design Codes and Cryptography, 2016.
- [16] D. Bernstein, J. Buchmann, and E. Dahmen, "Post-Quantum Cryptography," Springer, 2009.
- [17] K. S. Sahoo et al., "Blockchain-Based Secure Digital Asset Management System," IEEE Access, 2022.
- [18] Y. Liu et al., "Secure Smart Contract Framework for Blockchain Inheritance Systems," Journal of Network and Computer Applications, 2024.
- [19] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, 1978.
- [20] N. Koblitz and V. Miller, "Elliptic Curve Cryptography," Mathematics of Computation, 1985.
- [21] J. Katz and Y. Lindell, "Introduction to Modern Cryptography," CRC Press, 2020.
- [22] A. Menezes, P. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1996.
- [23] E. Rescorla, "SSL and TLS: Designing and Building Secure Systems," Addison-Wesley, 2001.
- [24] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," Wiley, 2015.
- [25] S. Singh, "The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography," Anchor Books, 2000.