Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 6, 2025

BLOCK CHAIN DRIVEN SUPPLY CHAIN SECURITY: INTEGRATING POST QUANTUM CRYPTOGRAPHY WITH AES

Eaman Raza Rizvi[*1], Shahzada Khurram[2]

[*1,2]*Department of Information Security, The Islamia University, Bahawalpur, Punjab, Pakistan.*

[*1]eaman.raza.rizvi@gmail.com, [2]khurram@iub.edu.pk

DOI: https://doi.org/10.5281/zenodo.15574111

Keywords
Etherum Block chain, Hybrid Encryption, Post Quantum Cryptography, Secure Data Interoperability, Supply Chain Security.

Article History
Received on 25 April 2025
Accepted on 25 May 2025
Published on 02 June 2025

Corresponding Author: *
Eaman Raza Rizvi

Abstract
Conventional cryptographic methods are gravely threatened by the development of quantum computing consequently, post quantum cryptographic (PQC) methods must be applied to secure data flow. In this work, we propose a hybrid encryption strategy based on Advanced Encryption Standard (AES) and Kyber, a lattice based PQC method, to raise the safety and processing efficiency of block chain systems, including multi stakeholders. Kyber codes keys Advanced Encryption Standard (AES) encrypts data. This approach lowers processing delay and is post quantum safe. Based on a performance study, the RSA encryption procedure takes 0.00049 seconds, and the decryption process takes 0.003051 seconds, therefore producing a total delay of 0.003524 seconds. Advanced Encryption Standard (AES) is quite efficient in generating a total delay of 0.000022 seconds, given a decryption time of 0.00001 seconds and an encryption time of 0.000012 seconds. The PQC hybrid (Kyber + AES) model helps one to reach these numbers with an encryption time of 0.0012 seconds, a decryption time of 0.0015 seconds, and a total processing delay of 0.002 seconds. This approach allows one to strike a compromise between real time communication effectiveness and safety. Research findings highlight the relevance of the concept in post quantum block chain systems, decentralized networks, and safe multiple party transactions, all settings where data integrity and secrecy are paramount. The paper presents a novelty in that it proved the existence of a hybrid encryption technique resistant to pragmatic and quantum computers.

INTRODUCTION

The implementation of secure data transmission security measures is mandatory in the current interconnected digital environment due to the escalating prevalence and complexity of cyber threats. Conventional encryption methods like the Data Encryption Standard (DES) [1] and the Rivest-Shamir-Adleman (RSA) algorithm have greatly helped digital communication's security. Still, traditional cryptographic techniques have fundamental limits including problems in scalability, complexity in key management, and sensitivity to the breakthroughs in quantum computing [2]. Furthermore, digital signatures assist to authenticate transactions while SHA-256 cryptographic hash codes provide data integrity verification [3]. Though they have some obvious benefits, block chain based security solutions struggle in speed and scalability. Hybrid encryption methods have been developed to increase effectiveness by combining the quick processing capacity of symmetric encryption for great data volumes with the strong security features of asymmetric encryption for key exchange [4]. New

cryptographic solutions include Elliptic Curve Cryptography (ECC) and quantum resistant encryption techniques considerably increase blockchain security by addressing potential quantum attacks [5]. Recently, block chain based supply chain management systems have been very popular as they increase transparency, traceability, and efficiency in environments with multiple stakeholders [6]. Still, these solutions largely depend on conventional encryption techniques, which are still susceptible to new cyberattacks. Including lattice based cryptography [7] post quantum cryptography (PQC) into blockchain networks shows a persuasive way to increase security by means of quantum resistant encryption algorithms. Sharding and off chain transactions under investigation now help to improve blockchain scalability [8]. Furthermore in research are quantum resistant cryptographic models and artificial intelligence driven security solutions meant to ensure that encryption methods remain robust against fresh cyber threats [9]. Reflecting the most current advances in the field, this study offers a hybrid encryption model integrating post quantum cryptography with AES to enhance secure data transmission in blockchain based supply chains. This hybrid method handles the challenges presented by advancements in quantum computing and AES for effective encryption by use of PQC based key exchange systems. This study tackles classical and quantum security concerns to enhance the development of block chain integrated encryption solutions for contemporary cybersecurity.

Literature Review

Block chain in Management of Safe Supply Chains Block chain technology is rising as a great answer for enhancing the security and transparency of supply chains. Traditional supply chains suffer as centralized control methods generate inefficiencies, lack of transparency, and security issues [10]. Block chain offers a distributed ledger assuring immutable record keeping, therefore reducing fraudulent activity and improving stakeholder interoperability. Many studies have shown, especially in multi stakeholder scenarios, how effectively block chain security of supply chain transactions holds [11]. Encryption Techniques Block chain based systems rely greatly on encryption techniques to maintain integrity and confidentiality. Though symmetric encryption methods such as Advanced Encryption Standard (AES) provide good data security, they rely on reliable key management [12]. Homomorphic encryption and zero knowledge proofs (ZKPs) are also looked at to provide privacy in block chain applications thereby enabling secure computations over encrypted data [13]. Post quantum cryptography (PQC) is thus required as traditional encryption techniques are becoming more vulnerable with quantum computing [14]. Relevance of Post Quantum Cyber security Post quantum cryptography (PQC) is a subject of cryptographic research seeking to produce algorithms resistant to quantum attacks. Effective breaking of widely used cryptography systems such as RSA and ECC by quantum computers especially those based on Shor's algorithm cause a considerable risk to existing encryption methods [15]. Groups like the National Institute of Standards and Technology (NIST) work to standardize by means of PQC as the next post quantum secure communication standard [16]. Safe supply chains benefit much from research in this area as PQC; by integrating block chain ensures long term security and trust in distributed systems. Encrypted Hybrid Block chain Techniques Combining the best features of symmetric and asymmetric encryption, hybrid encryption offers economy and security [17]. Hybrid encryption approaches mix symmetric encryption for quick data processing with asymmetric encryption for safe key exchanges in block chain systems [18].

Methods/Materials

This section provides the methodological background for creating a block chain based hybrid encryption model integrating Post Quantum Cryptography (PQC), hence improving safe data exchange in a multi stakeholder supply chain. The suggested method combines PQC for robustness against quantum attacks with the distributed architecture of block chain with symmetric encryption for data secrecy. One guarantees safe, scalable, and interoperable data sharing by way of a methodical approach including system architecture design, cryptographic protocol selection, and block chain deployment. The technique guarantees its relevance in real world supply chain contexts

encompassing many stakeholders by tackling important security and communication issues.

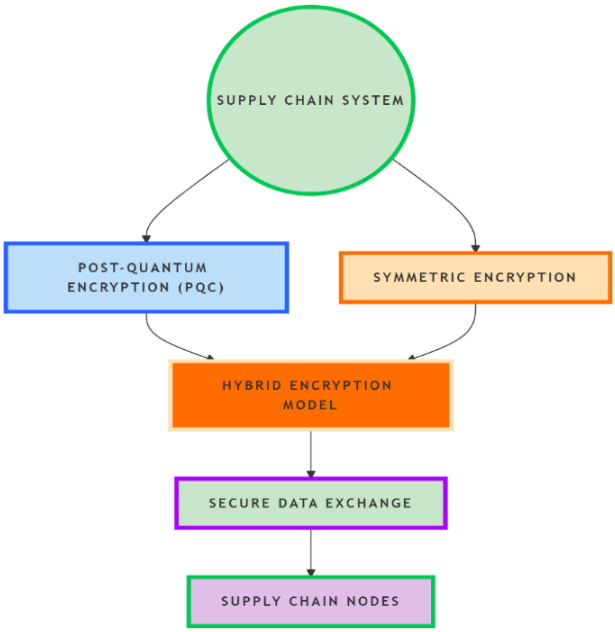

Figure 1. Flow chart of our proposed model

How work Hybrid Approach

PQC Safe Key Exchange Cryptography

Using lattice based encryption and other quantum resistant cryptographic techniques; PQC encrypts the symmetric AES key hence ensuring a secure key exchange mechanism. Unlike traditional asymmetric encryption systems like RSA, which are prone to quantum computing attacks, PQC-based approaches provide enhanced security by avoiding key compromise. This approach strengthens hybrid encryption models against evolving cyber security problems, hence ensuring long term data protection in the framework of increased quantum computing powers.

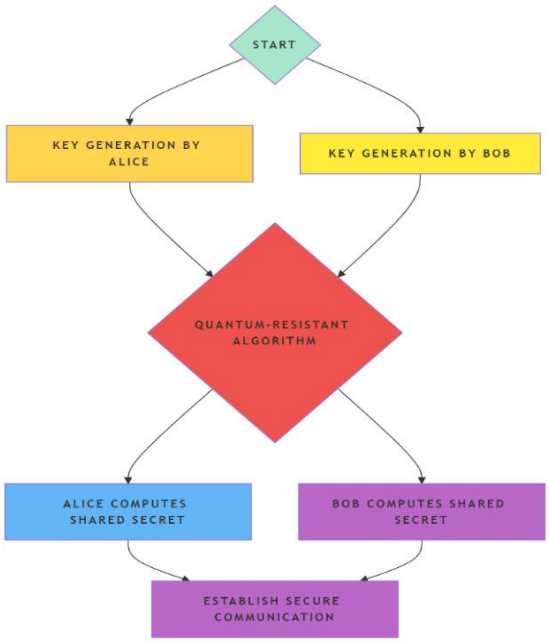

Figure 2. Key exchange flow work diagram.

Algorithm 1. Post-Quantum Secure Key Exchange Algorithm
Input: Client Key Pair ($SKClient, PKClient$), Server Key Pair ($SKServer, PKServer$)
Output: Shared Secure Session Key
Step 1: Key Generation
Client generates PQC key pair ($PKClient, SKClient$)
Server generates PQC key pair ($PKServer, SKServer$)
Step 2: Key Exchange
Client sends $PKClient$ to Server
Server sends
$PKServer$ to Client
Step 3: Key Derivation
Compute shared key: KShared = PQC Key Exchange ($PKClient, SKServer$)
Client computes the same key: KShared = PQC Key Exchange ($PKServer, SKClient$)
Step 4: Secure Session Established
if *KShared is valid* ***then***
Begin Secure Communication
end
else
Reject Connection and Restart Handshake
end

Hybrid Encryption Strategy Development AES lattice based

In the proposed hybrid encryption system, PQC for key encryption combined with AES for data encryption provides protection against both conventional and quantum attackers. Originally meant to encrypt the data, AES is a symmetric encryption technique offering excellent economy and security. Then PQC more precisely, lattice based cryptography locks the AES encryption key to provide resistance against quantum attacks. Following that, encrypted data and keys are combined into one package under cryptographic hash techniques to verify data integrity. This encrypted package is stashed securely and delivered across the Ethereum block chain, which offers immutability and smart contract tools for safe access control. The receiver decodes the data using AES during decryption first obtaining the AES key using their PQC private key. By ensuring that the confidentiality and integrity of the data stay preserved even if one encryption layer is compromised, this tier of encryption helps to improve security. Combining PQC for secure key exchange with AES for efficient data encryption provides powerful security architecture able to withstand advancements in quantum computing. Moreover enhancing security is the Ethereum block chain, which provides distributed storage and controlled data access thus ensuring data integrity and resistance against unauthorized alterations. For main uses that maintains processing efficiency and long term cryptographic resilience, this approach provides a reasonable option

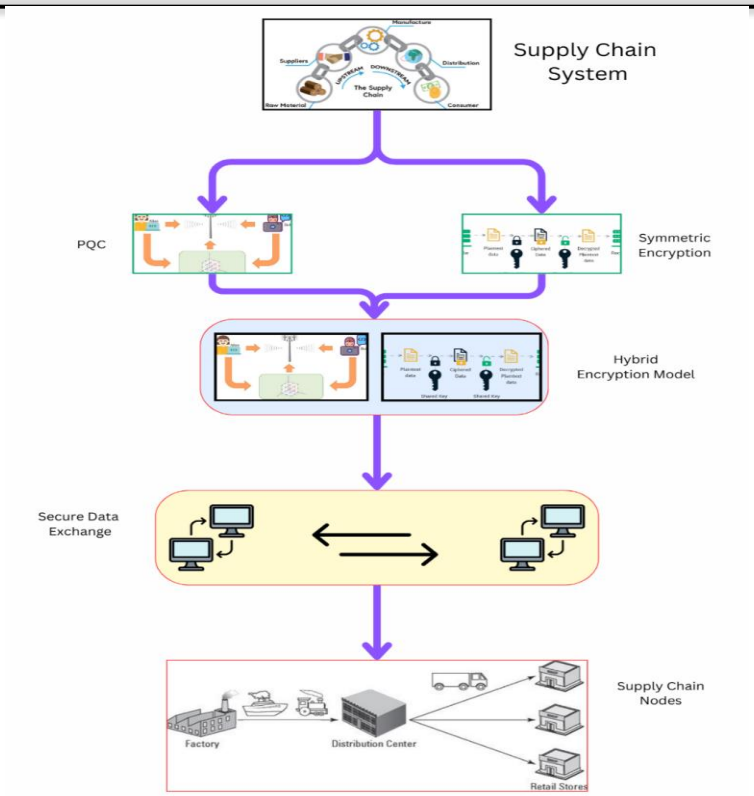

Figure 3. Hybrid Encryption Strategy Development AES lattice based

Algorithm 2. PQC Hybrid Encryption for Secure Blockchain Transmission
Step 1: Key Generation
Generate AES symmetric key KAES
Generate PQC key pair (PKPQC,SKPQC)
Generate digital signature key pair (SKSign,PKSign)
Step 2: Encrypt Data for Confidentiality
Encrypt data D using AES: C = AES Encrypt(KAES,D)
Encrypt AES key using PQC: CK = PQC Encrypt(PKPQC,KAES)
Step 3: Generate Digital Signature for Integrity
Compute hash of encrypted data: H = Hash(C)
Sign the hash using private key: Sig = Sign(SKSign,H)
Step 4: Transmit Secure Transaction Over Blockchain
Create transaction T = (C,CK,Sig,PKSign)
Append transaction T to blockchain ledger: Blockchain Ledger ← Blockchain Ledger ∪ T
Step 5: Receiver Verification and Decryption
Retrieve transaction T from blockchain
Verify signature: H' = Hash(C) if Verify (PKSign,Sig,H') = False then
Reject Transaction: Integrity compromised
return Failure
Decrypt AES key: K'
= PQC Decrypt(SKPQC,CK)
Decrypt data: D' = AES Decrypt(K'
Step 6: Validate Integrity if D′ = D then
Accept Transaction: Data is secure and unaltered return Success else
Report Tampering: Data integrity violated return Failure

Storing on Ethereum Block chain

Beyond digital transactions, Ethereum block chain is a distributed application (dApps) and smart contract creation facilitative decentralized and programmable platform that helps supply chain management and other developments. Among its main parts is the Ethereum Virtual Machine (EVM), which guarantees security, openness, and immutability by allowing smart contracts to run. By choosing validators based

on pledged assets rather than processing capability, Ethereum's shift to a Proof-of-Stake (PoS) consensus method improves scalability and energy efficiency. Ethereum transactions pay validations for network security and computing resources gas costs, expressed in Ether. Ethereum records transactions in an unchangeable way as a distributed ledger, therefore encouraging openness and responsibility in supply chains.

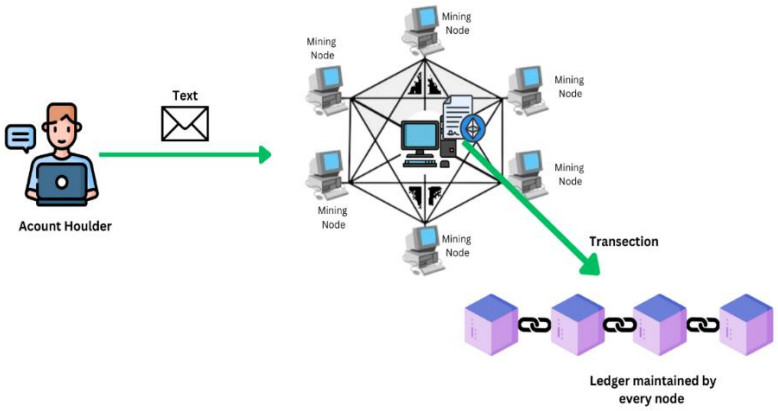

Figure 4. Storing on local Etherum block chain

Message Verification using hash based signatures

A fundamental component of Post Quantum Cryptography (PQC), hash based signatures (HBS) guarantees data integrity and authenticity against quantum computing threats. Whereas RSA and Elliptic Curve Cryptography (ECC) depend on number theoretic hardness assumptions susceptible to Shor's algorithm, HBS generates safe digital signatures using cryptographic hash functions (e.g., SHA-256, SHA-3). Long-term security uses include government communications, financial transactions, and block chain based systems find HBS especially appropriate for their quantum resilience

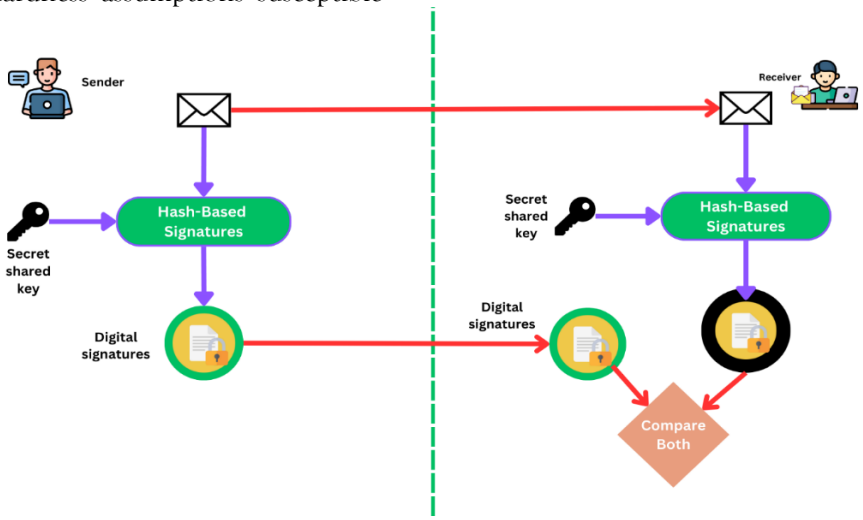

Figure 5. Identity verification

Evaluation matrices

To guarantee resistance against both conventional and quantum computing threats, the assessment of Post Quantum Cryptography (PQC) based hybrid systems needs a thorough study of security, integrity, performance, scalability, and energy economy.

Applications like block chain technology and safe data transfer, where long term cryptographic security is crucial, depend especially on these elements.

Security

PQC hybrid systems have to show resistance against quantum attacks, especially those using Shor's and Grover's algorithms, which endanger conventional cryptography techniques as RSA and Elliptic Curve Cryptography (ECC). Strong quantum resistant substitute lattice based encryption guarantees safe key exchange and encryption. Protection of data integrity and avoidance of man in middle attacks depend critically on authentication systems like quantum resistant digital signatures and hash-based message authentication codes (HMACs).

Performance

$$P = D / T \quad (1)$$

where P implies performance, D is data size, and T is processing time.

A reduced latency improves system efficiency, which is expressed by

$$P = 1 / L \quad (2)$$

where L denotes delay.

Scalability

Scalability gauges whether the system can maintain computational efficiency while managing growing user expectations and data quantities. PQC algorithms can need more significant key sizes, therefore their effect on processing performance and computational overhead has to be investigated. Modelling the expected processing time for growing data amount, we find:

$$T(n) = T_0 + k \cdot n \quad (3)$$

denotes the total processing time for data size n by means of T_0 as the base processing time and k as the time complexity per unit data.

Integrity

PQC hybrid systems' first priority is data integrity. SHA-256 and SHA-3 cryptographic hash mechanisms preserve data authenticity and detect illegal changes.

$$I = 1 - Pf \quad (4)$$

where I stands for integrity and P_f is the likelihood of data modification we can measure the probability of integrity violation.

Energy Consumption

Large scale cryptographic processes, particularly in block chain based systems, give great weight to energy economy. A cryptographic operation's total energy consumption is found by

$$E = P_avg \times t \quad (5)$$

where E is the total energy in joules, P_avg is the average power consumption, and t is the operating time.

Calculating the energy per operation,

$$E_op = P_total/N \quad (6)$$

uses P_total as the total power spent against N as the number of cryptographic operations.

Results / discussion

This study offers a hybrid encryption method combining Post Quantum Cryptography (PQC) with Block chain technology to improve data interoperability in multi stakeholder supply chains. Strong security measures are very vital given the growing complexity of supply chains. Using AES and lattice based PQC to address quantum concerns; our method combines symmetric and asymmetric encryption. Extensive assessments show that the suggested architecture improves data privacy, encryption efficiency, and system resilience, therefore providing a workable option for safe supply chain management. The security study of cryptographic algorithms includes PQC hybrid approaches, AES, and RSA offers understanding of their efficiency in protecting digital systems. Whereas AES is well known for its speed and efficiency in symmetric encryption, RSA depends on the computational difficulties of factoring big integers for public key encryption. Resilience against quantum attacks makes hybrid methods combining Post Quantum Cryptography (PQC) more and more valuable. Based on encryption strength, performance, and security against quantum computing, this paper contrasts different methods emphasising their viability in present and future cryptographic settings.

RSA Algorithm Strength

Algorithm Strength RSA is successful yet, it is susceptible to threats from quantum computers. While it is still strong in conventional environments (8/10), developments in quantum computing provide a major concern.

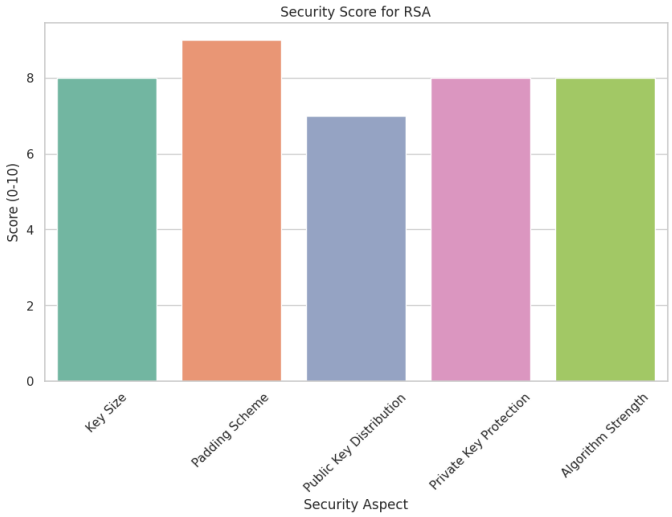

Figure 6. Graph shows the security score of RSA with different aspects

AES Algorithm Strength

Security strength

An Advanced Encryption Standard review is on its computational economy, security, and efficiency. Because of its quick encryption and decryption features, AES is increasingly used in real time applications. Crucially in hybrid encryption systems, it offers great security with little computational cost with key sizes of 128, 192, or 256 bits. AES shows great security in many spheres. With specified key sizes, it provides strong encryption that reduces computing effort and guarantees good defence against brute-force assaults. OAEP and other secure padding systems improve resilience to ciphertext assaults; however, safe key management is still crucial to avoid weaknesses.

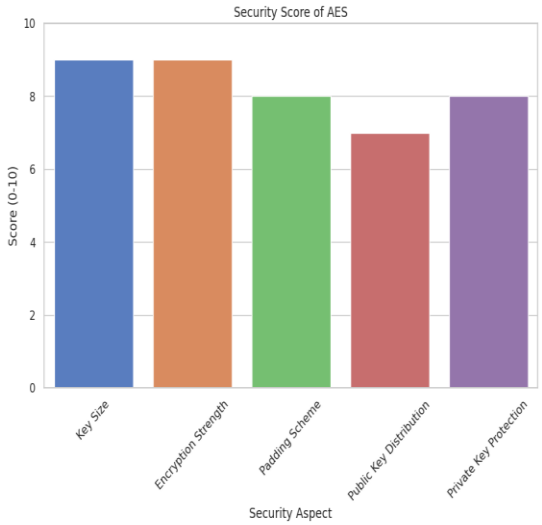

Figure 7. Security graph of AES with different aspects

Hybrid (AES + Kyber 512) Results

Key size & security

• Key Size: Kyber-512 makes use of a big key size (1–2 KB) in contrast to conventional encryption techniques like RSA or AES by itself. Greater security from larger key sizes helps to make one very resistant to brute force assaults.

• Encryption Strength: Kyber, a post quantum cryptographic system, is combined with AES, a symmetric encryption method in a hybrid manner. Kyber is designed to resist quantum assaults, therefore guaranteeing long term security.

• Kyber's padding system strengthens security against selected plaintext attacks (CPA). Additionally using safe padding techniques helps AES stop data leaks.

• Kyber-512 makes use of lattice-based encryption, which enables safe public key exchange free from weaknesses like those in RSA (which is vulnerable to Shor's quantum algorithm).

• While Kyber's architecture reduces the danger of private key exposure, AES guarantees strong private key security, therefore providing a very safe hybrid method.

With a 9.5/10 security score, the PQC Hybrid approach's protection of data from both conventional and quantum threats shows.

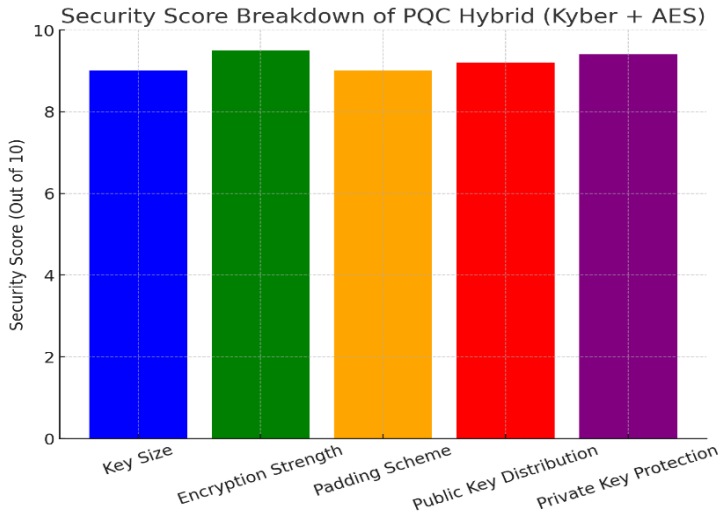

Figure 8. Security score of PQC + AES approach

Comparison of PQC Hybrid (AES + Kyber 512) Encryption with RSA and AES

Particularly given the development of quantum computing hazards, the choice of encryption techniques greatly affects data security and speed. Three cryptographic methods Post Quantum Cryptography (PQC) using Kyber 512 and AES, RSA (asymmetric encryption), and AES (symmetric encryption) are compared in this work. Data size, encryption strength, performance, and security comprise the main points of comparison.

Data Size and Encryption Strength

Cipher text size, key length, and security vary throughout encryption methods. RSA depends on huge key lengths for security, so it creates big cipher texts. While the PQC hybrid technique guarantees quantum resistance by mixing AES with Kyber 512, as a symmetric method AES is more space efficient.

- RSA With a matched key size of 256 bytes, RSA generates a much bigger cipher text (256 bytes) using its asymmetric encryption method. It is thus susceptible to future quantum assaults because it lacks quantum resistance.
- AES is efficient for encryption as its key and cipher text size 32 bytes are substantially less. Grover's method may thus weaken its security strength, so it is only somewhat immune to quantum assaults.
- PQC Hybrid (Kyber + AES) Kyber's lattice-based encryption causes PQC Hybrid (Kyber + AES) to introduce a much bigger cipher text size (1-2 KB)

and key size (1-2 KB). Though at the expense of more storage and transmission overhead, this guarantees strong security against quantum attacks; hence it is a suitable option for post quantum cryptographic uses.

Table 1. Data size, cipher text size of each algorithm

Technique	Data Size	Ciphertext Size	KeySize	Quantum Resistance
RSA	18	256	256	No
AES	18	32	32	Partially
PQC Hybrid	18	1-2 KB	1-2 KB	Yes

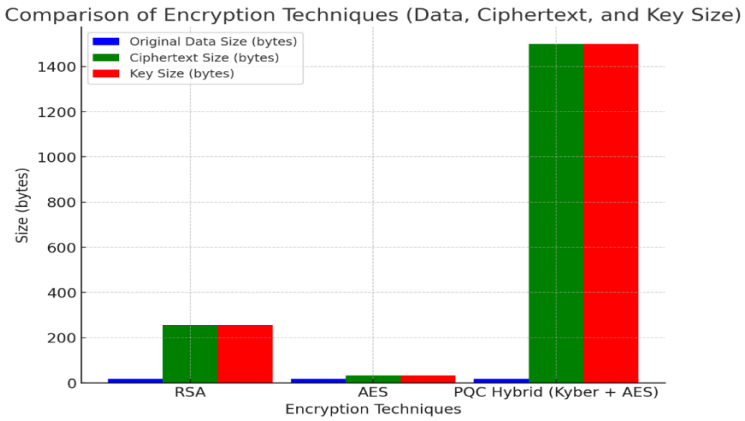

Figure 9. Comparison graph of RSA, AES and PQC hybrid approach of key size, cipher text and data.

Performance

Performance analysis covers delay, encryption and decryption times. While AES offers quick encryption, RSA shows more computational latency. With a reasonable latency, the PQC hybrid approach strikes a compromise between security and performance.

Table 2. Latency and performance of AES, RSA and hybrid PQC

Technique	Encryption Time (s)	Decryption Time (s)	Latency (s)
RSA	0.001176	0.001528	0.002704
AES	0.000018	0.000010	0.000028
PQC Hybrid	0.0009 - 0.0012	0.0009 - 0.0015	0.002

Security Score

While AES offers great resistance against classical threats but remains vulnerable to Grover's method, RSA is vulnerable to quantum assaults. High security against quantum attacks is provided by the PQC hybrid technique with Kyber 512.

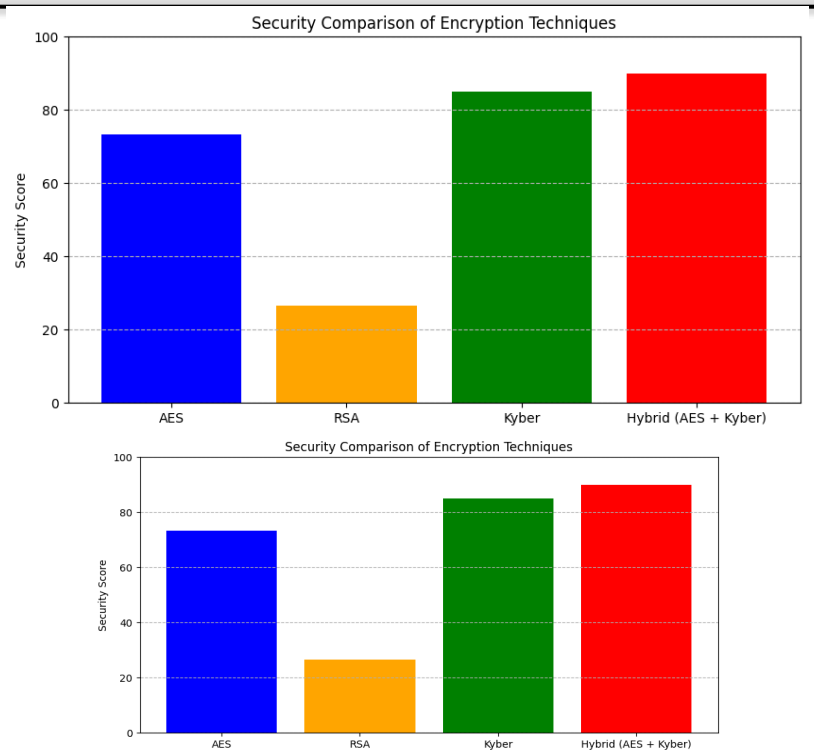

Figure 10. Security comparison of AES, RSA and PQC hybrid

Vulnerabilities and Mitigation

RSA faces security risks from quantum algorithms, large key sizes, high latency, and scalability issues. The PQC hybrid approach mitigates these vulnerabilities through quantum resistance, optimized key sizes, lower latency, and future proof scalability.

Table 3. Vulnerabilities and Mitigation

Vulnerability	RSA + AES Vulnerability	PQC Hybrid Mitigation	Vulnerability
Quantum Vulnerability	RSA vulnerable to Shor's Algorithm	Kyber 512 is quantum resistant	Quantum Vulnerability
Key Size Overhead	Large key sizes for security (e.g., 3072-bit)	Smaller key sizes (1-2 KB) for better efficiency	Key Size Overhead
Latency in Real Time Systems	High latency due to RSA decryption	Lower latency with faster Kyber 512 decryption	Latency in Real Time Systems
Scalability Issues	RSA requires larger keys for higher security	Kyber 512 scales securely without large key sizes	Scalability Issues

G. Transaction data visualization local Ethereum Block chain

A bar chart shows the Ethereum (ETH) exchanged in each transaction (Tx-1 to Tx-7) on the Transaction Amounts graph (top plot). A line graph shows the seconds taken for every transaction in the Transaction Durations graph (bottom plot). At around one second, Tx-1 has the lowest length Tx-3 and Tx-5 displays the largest durations roughly three seconds. Between two and two 5 seconds span the remaining transactions Tx-2, Tx-6, and Tx-7. Larger transactions (e.g., Tx-4) do not always require longer durations, so the two graphs emphasize both the changes in transaction amounts and the related durations, thereby revealing a non linear connection between transaction size and time.

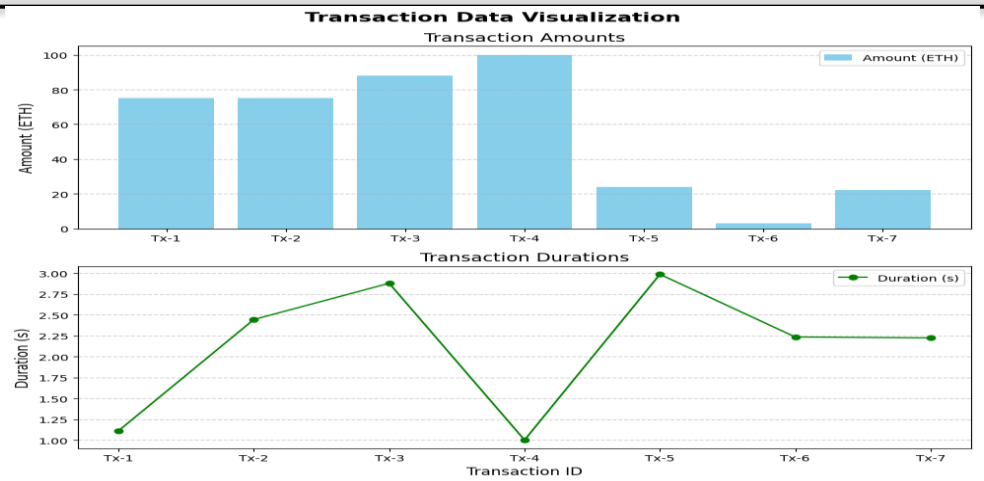

Figure 11.Transaction data visualization local Ethereum Block chain

Successful Transactions visualization

Successful Transactions of two accounts shown in this screen short.

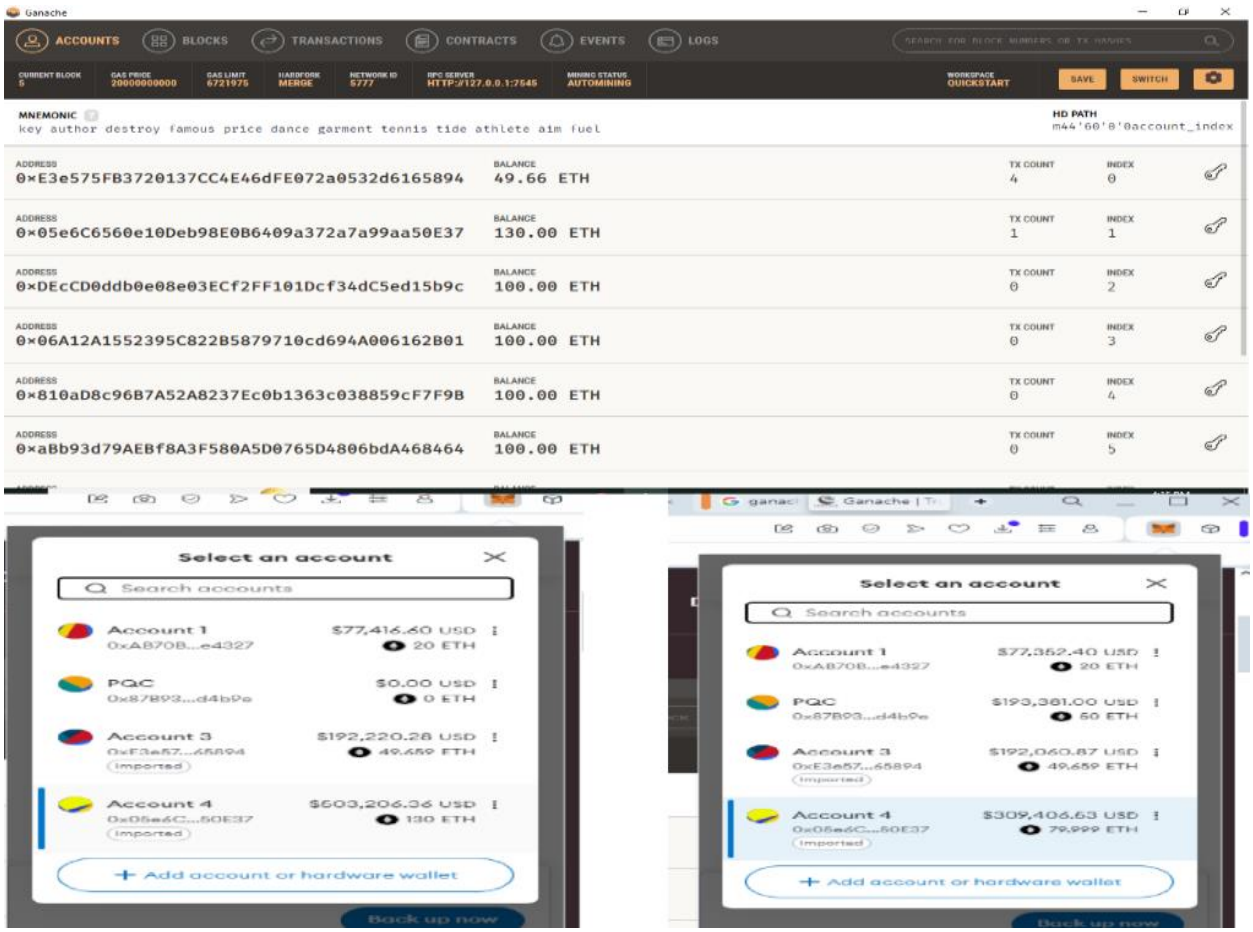

Figure 12. Successful transactions visualization

H. Conclusion

Comparative analysis of encryption systems reveals that while effective, conventional approaches like RSA and AES lack quantum resistance and so are susceptible to future cryptographic attacks. Strong security assurances against quantum assaults arise from PQC based methods, but they also raise scaling issues and processing expenses. Combining the dependability of PQC with the efficiency of symmetric encryption, hybrid encryption models provide a balanced solution for safe multi stakeholder block chain systems. Optimizing hybrid encryption methods should be the main emphasis of further studies to guarantee flawless block chain integration, lower computational cost, and improve speed. Solving these issues would help hybrid PQC based. Although hybrid encryption methods as Post Quantum Cryptography (PQC) show great promise in safeguarding block chain based multi stakeholder systems, many important issues have to be resolved to guarantee useful deployment Lattice based PQC systems affect block chain node performance by adding significant computational cost. Hardware acceleration e.g., FPGA, GPU based implementations and software level optimizations to improve efficiency should be investigated in further studies. Scalability and Transaction Throughput: PQC's inclusion into block chain systems has to maintain high transaction speeds. Investigated should be optimized cryptography protocols and compression methods to reduce the influence on block chain scalability. Prevention of vulnerabilities in hybrid encryption systems depends on safe key distribution, storage, and retrieval techniques. Block chain based Decentralized Key Management Systems (DKMS) might be a good fix. Widespread use requires seamless integration of PQC with block chain systems as Ethereum and Hyper ledger, which already exist. Designing flexible cryptographic modules that fit current consensus processes and smart contract systems should be the main priorities of further research.

REFERENCES

[1] Zhou, Z., & Liu, Y. (2022). Blockchain-Based Encryption Method for Internal and External Health Privacy Data of University Physical Education Class. Journal of Environmental and Public Health, 2022(1), 7506894.

[2] Likhita, M., Ravindranath, K., Vaishnavi, G., Dabhi, V., & Teja, A. S. (2024). Hybrid Cryptography Model To Enhance The Security In Cloud.

[3] Chen, Z., Gu, J., & Yan, H. (2023). HAE: A Hybrid Cryptographic Algorithm for Blockchain Medical Scenario Applications. Applied Sciences, 13(22), 12163.

[4] Samy, I. A. A., & Mary, M. S. (2022). Secure Data Transmission in Cloud Computing Using Std-RSA With Eslurnn Data Classification and Blockchain Based User Authentication System.

[5] Li, J., Sun, Q., & Sun, F. (2023). Enhancing Privacy-Preserving Intrusion Detection in Blockchain-Based Networks with Deep Learning. Data Science Journal, 22(1).

[6] Likhita, M., Ravindranath, K., Vaishnavi, G., Dabhi, V., & Teja, A. S. (2024). Hybrid Cryptography Model To Enhance The Security In Cloud.

[7] Pandian, R. S. R., & Columbus, C. (2022). An analytical approach for optimal secured data storage on cloud server for online education platform. Geoscientific Instrumentation, Methods and Data Systems Discussions, 2022, 1–36.

[8] Neelakandan, S., Beulah, J. R., Prathiba, L., Murthy, G., Irudaya Raj, E. F., & Arulkumar, N. (2022). Block chain with deep learning-enabled secure healthcare data transmission and diagnostic model. International Journal of Modeling, Simulation, and Scientific Computing, 13(04), 2241006.

[9] Cosseron, O., Hoffmann, C., Méaux, P., & Standaert, F.-X. (2022). Towards case-optimized hybrid homomorphic encryption: Featuring the elisabeth stream cipher. International Conference on the Theory and Application of Cryptology and Information Security, 32–67.

[10] Jayaprakash, V., & Tyagi, A. K. (2021). Security optimization of resource-constrained internet of healthcare things (IOHT) devices using asymmetric cryptography for blockchain network. International Conference on Network Security and Blockchain Technology, 225–236.

[11] Wenhua, Z., Qamar, F., Abdali, T.-A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: Security issues, healthcare applications, challenges and future trends. Electronics, 12(3), 546.

[12] Alzoubi, Y. I., Al-Ahmad, A., Kahtan, H., & Jaradat, A. (2022). Internet of things and blockchain integration: Security, privacy, technical, and design challenges. Future Internet, 14(7), 216.

[13] Aggarwal, S., & Kumar, N. (2021). Basics of blockchain. In Advances in computers (Vol. 121, pp. 129–146). Elsevier.

[14] Odulaja, B. A., Ihemereze, K. C., Fakeyede, O. G., Abdul, A. A., Ogedengbe, D. E., & Daraojimba, C. (2023). Harnessing blockchain for sustainable procurement: Opportunities and challenges. Computer Science & IT Research Journal, 4(3), 158–184.

[15] Gucciardi, A. (2023). Trustless contract management: A study on the benefits of blockchain-based smart contracts [PhD Thesis]. Politecnico di Torino.

[16] Junaid, L., Bilal, K., Shuja, J., Balogun, A. O., & Rodrigues, J. J. (2024). Blockchain-Enabled Framework for Transparent Land Lease and Mortgage Management. IEEE Access.

[17] Shakor, M. Y., Khaleel, M. I., Safran, M., Alfarhood, S., & Zhu, M. (2024). Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security. IEEE Access.

[18] Maalavika, S., Thangavel, G., & Basheer, S. (2024). Performance Evaluation of RSA Type of Algorithm with Cuckoo Optimized Technique. 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), 5, 1362–1367.