

VishwasQ: a decentralized post-quantum trust framework for secure IoT-enabled smart parking networks

Aditya Patadiya¹, Utsav Savaliya¹, Yuvraj Jadav¹, Om Prakash Suthar¹, Sushil Kumar Singh^{1*}  and Hoi Leong Lee²

¹ Department of Computer Engineering, Marwadi University, Rajkot, Gujarat 360003, India

² Faculty of Electronic Engineering and Technology, Universiti Malaysia Perlis, Arau, Perlis 02600, Malaysia

* Correspondence: sushilkumar.singh@marwadieducation.edu.in (Singh SK)

Abstract

Smart parking systems are an application of advanced mobility; however, they face several challenges, including security, privacy, and transaction integrity, especially in the era of quantum computing. This paper proposes VishwasQ, a decentralized post-quantum trust framework for secure IoT (Internet of Things)-enabled smart parking networks that integrates Post-Quantum Cryptography (PQC), Blockchain Technology (BT), and Ethereum-based smart contracts (SC) to enable quantum-resistant confidentiality and decentralized trust. PQC-based encryption is utilized to secure user and payment data prior to storage in a MySQL backend, while Firebase authentication is employed for efficient user identity management. At the third layer, immutable audit maintenance, payment processing, and penalty enforcement are automated through smart contracts. The proposed framework also utilizes QR code-based access control for efficient entry and exit validation, thereby reducing fraud and enhancing usability. Experimental evaluation demonstrates promising performance, with PQC encryption introducing approximately 15% overhead compared to RSA (Rivest–Shamir–Adleman Cryptosystem), an average Ethereum test-net transaction latency of 15 s, and QR code validation within 2 s. The framework achieves 100% success in enforcing penalties through smart contracts, while maintaining an average gas consumption of 0.00021 ETH (Ether [Ethereum Cryptocurrency]) per booking transaction, indicating cost-effectiveness for practical deployment. These results highlight that the proposed framework provides quantum-resilient security, tamper-proof auditing, and automated financial transparency with minimal performance overhead, outperforming existing research studies.

Keywords: Post-Quantum Cryptography, Smart parking system, Blockchain, Smart contracts, Ethereum, QR code authentication, Data security, Decentralized systems

Citation: Patadiya A, Savaliya U, Jadav Y, Prakash Suthar O, Singh SK, et al. 2026. VishwasQ: a decentralized post-quantum trust framework for secure IoT-enabled smart parking networks. *Digital Transportation and Safety* 5(3): 318–329 <https://doi.org/10.48130/dts-0026-0025>

Introduction

The rapid development of urbanization and the significant increase in the number of automobiles have created a binding need for secure, efficient, and transparent parking management procedures in contemporary smart cities. Although conventional parking systems encourage users to book slots and pay online, several limitations persist, including manual slot management, insufficient security in payment media, limited transparency, and vulnerability to network and cyberattacks. This reliance on centralized or third-party servers and traditional public-key cryptographic methods, such as RSA, Secret Sharing, and ECC (Elliptic Curve Cryptography), further exposes these systems to risks of data breaches, centralization, and scalability issues^[1]. More significantly, improvements in quantum computing pose a serious threat, as algorithms such as Shor's algorithm can potentially break RSA, Secret Sharing, and ECC, making existing cryptographic techniques unsuitable for forthcoming smart city applications. The elaboration of intelligent parking systems reflects not only advancements in digital and smart infrastructure but also the growing need for collaborative advanced innovations to address emerging security attacks and scalability challenges. The extensive use of IoT-based sensors, remote analytics, and seamless digital smart payment solutions has enabled cities to optimize slot utilization and traffic direction. However, persistent challenges, such as evolving cyber threats, inadequate regulatory frameworks, and increasingly sophisticated attack mechanisms,

remain unresolved. As cities become more interconnected and mobility needs continue to evolve, smart parking^[2] is emerging as a critical testbed for integrating advanced research studies in cryptography, network security, and automated enforcement to secure reliability, fairness, and future readiness across diverse smart environments. In this context, collaboration among academia, industry, and government workers is essential.

While blockchain enhances transparency and security against tampering, it does not guarantee the privacy of the information being shared among the users, IoT devices, and backend servers. The majority of the current smart parking systems still use traditional public-key cryptographic methods like RSA and ECC for authentication and secure communication. While these cryptographic schemes are believed to be secure against classical computers, they fall apart in the face of powerful quantum computers, since Shor's algorithm can solve the mathematical problems behind which RSA and ECC are designed in an efficient way. Smart city infrastructures and IoT deployments are usually deployed for many years^[3], and so the information collected today may be stored and accessed by future adversaries using quantum computers ('harvest now, decrypt later'). Therefore, implementing Post-Quantum Cryptography has become a necessity, as it ensures long-term confidentiality, secure authentication, and robust communication in smart parking systems while maintaining the decentralized trust and security that blockchain technology offers^[4].

Motivation

In spite of these technological innovations, there is still a fundamental vacuum in the assurance of future-proof security and trust in the smart parking system^[5]. The accumulation of new dangers in unified and globalized city spaces, such as quantum-enabled cryptanalyses of classical cryptosystems, more advanced cyberattacks on centralized infrastructure, etc., calls for architectural solutions both visionary and practical. To ensure strong security of sensitive user data, integrity of high-value financial transactions, and to provide uninterrupted experiences, quantum-resistant cryptographic protocols^[6], decentralized trust systems, and automatic validation systems should be combined. These multidimensional challenges must be dealt with not only in the protection of the current urban mobility infrastructure but also in the protection of the scalability and resilience of cities in the quantum era. We propose integrating a post-quantum secure smart parking system design with numerous contemporary technologies to ensure quantum resilience and operational transparency. The system uses a lattice-based post-quantum cryptography (PQC) technique^[7,8] to encrypt sensitive user and vehicle data and store it in a MySQL database. Firebase user authentication and identity management ensure scalable and dependable frontend integration. The design uses blockchain to preserve the audit trail of all booking and payment operations to prevent tampering and fraud. Ethereum-based smart contracts with Solidity code allow slot labelling, payment confirmation, overtime penalty computation, and refunds without third-party intervention. QR code validation ensures safe and efficient parking facility admission and exit, and links access control to blockchain transactions. A prototype and Ethereum testnet were used to test the framework. These studies show that PQC has a 15% computational cost over RSA, is quantum-safe, blockchain has immutable records, has a mean transaction delay of 15 s, and QR validation takes under 2 s. Smart contracts automate payments and penalties with 100% success, and the average gas cost was 0.00021 ETH per booking transaction, proving they can be used in urban areas.

PQC has several noteworthy features over traditional cryptographic methods, particularly for Next-Generation smart parking systems. First, lattice-based PQC algorithms are efficient, both classically and quantumly, and suitable for use in server-side and IoT-assisted deployments. Second, PQC can be employed to securely establish keys for booking data, payment data, and user identities, without relying on cryptographic assumptions that are questionable in the quantum era. Third, the integration of blockchain with PQC forms a complementary security system that ensures transparency and data integrity through blockchain while providing confidentiality and secure communication via PQC. This combined solution provides a future-proof security solution that can be used for long-term deployments of a smart city without any significant architectural changes once quantum computing is practically available.

Contributions

The proposed research presents a new decentralized and quantum-resistant trust framework called VishwasQ for secure smart parking systems using IoT devices. The framework combines some new technologies, such as PQC and blockchain technology, with Ethereum smart contracts and QR code-based access control in a unified architecture to achieve the aim of providing confidentiality, integrity, transparency, and automatic trust management at the same time. The key achievements of this work are outlined as follows:

- The first integrated quantum-resilient trust framework for IoT-enabled smart parking, using a combination of lattice-based post-quantum cryptography, blockchain technology, Ethereum smart contracts, and QR-code validation within a single end-to-end architecture.
- Fills a crucial gap in research by securing smart parking infrastructures from classic and quantum attacks, while the majority of current parking systems based on blockchain remain based on traditional public-key cryptography methods like RSA or ECC.
- Creates a hybrid architecture with multiple layers that include frontend services, secure backend storage, blockchain-based auditing, and access control via IoT, offering decentralized trust, data confidentiality, and transparency.
- Automates parking reservations, processing of payments, management of refunds, and ensures penalties for overstaying time without the need for centralized authorities or third-party intermediaries by implementing Ethereum smart contracts.
- Embeds blockchain-verified QR-code access control into vehicles to ensure secure entry and exit while also tying physical access to vehicles to immutable blockchain transaction records.
- Comprehensive prototype implementation and experimental evaluation, analysis of post-quantum cryptographic overhead, blockchain latency, gas consumption, QR-code validation time, and overall system performance, providing evidence that quantum-resistant security can be attained with acceptable computational overhead for smart city deployments in practice.
- Shows that PQC can be practically deployed in conjunction with blockchain for real-world smart parking applications, offering a future-proof architecture that can support next-generation intelligent transportation and smart city ecosystems.

Organization

The rest of the article is structured in the following way: section "Related works" introduces related work of existing research, and the primary consideration of the proposed architecture; section "Decentralized post-quantum trust framework for secure IoT-enabled smart parking networks" provides the in-depth system architecture and workflow of the suggested smart parking system. Section "Performance evaluation and analysis" explains the performance analysis and the results of the experiment, and the last section "Conclusions" provides the paper with limitations and future work directions.

Related works

This section discusses the seminal contributions of existing works with a comparison table and the requirements of the proposed framework, and shows how to address the limitations of the existing works with the proposed framework.

Seminal contributions

The literature regarding secure parking systems based on blockchain, artificial intelligence, and cryptography is increasing. Ankarboina et al.^[9] proposed an SQL-based smart parking system fused with ECC, AES-GCM (Advanced Encryption Standard–Galois/Counter Mode), and JWT (JSON Web Token) for lightweight and secure communication and addressed various challenges, such as response authentication and replay protection approaches. Experimental results of the research studies demonstrated improved efficiency, achieving higher throughput and reduced registration delay

compared to existing methods. Still, trust and centralization are issues in this research study. Singh et al. came up with PARK Tag, the AI-blockchain integrated smart parking system, which is designed to streamline city mobility via slot prediction and safe transactions. Although this work is efficient in terms of slot allocation, it is silent on quantum-resilient security, exposing data and transactions to the risk of being attacked by quantum computers in the future^[10]. Zhang et al. proposed a smart parking system based on the blockchain IoT framework that uses smart contracts to manage it decentrally and ensure payment automation. Their solution is transparent and immutable for parking records, yet it lacks the post-quantum security needed to be resilient over the long term. Other works in this area have concentrated mainly on the aspects of decentralization and transparency without considering the threats of the quantum era^[11]. Vijayalakshmi et al.^[12] proposed an intelligent smart parking system merged with an Intrusion Detection System (IDS) for VANET (Vehicular Ad Hoc Networks) environments. The main objective of this research is to ensure secure and efficient parking management using IoT and sensor data and to prevent cyber threats, particularly DDoS attacks, through a machine learning-based IDS using an LSTM model. The system demonstrated high effectiveness, achieving 97% accuracy in attack detection and improving structured parking operations. Its merits include enhanced security, efficient space utilization, and preference-based access control. However, limitations include potential computational overhead, dependency on ML model training quality, and limited scalability evaluation in large real-world deployments. Alymani et al.^[13] proposed a smart parking system using ANPR (Automatic Number Plate Recognition) and OCR (Optical Character Recognition)-based license plate recognition, along with camera-based detection of empty parking areas to enhance advanced parking efficiency. The objective of this research study is to reduce time, fuel wastage, and manual intervention by automating vehicle authentication and real-time parking availability, and the advantage of this research is to include enhanced user convenience, reduced congestion, improved security, and efficient space utilization. However, there are challenges to this research study, including dependence on camera accuracy, potential security and privacy concerns, and handling poor lighting or weather conditions impacting the recognition arrangement.

In the field of cryptography, researchers have examined post-quantum cryptography (PQC)^[14] within the context of the Internet of Things (IoT). Lattice-based (e.g., Kyber) and stateless hash-based (e.g., SPHINCS+) signature schemes have become viable proposals for resource-constrained devices thanks to their high security levels and manageable performance overheads. In a work by Liu et al., QBIoT is a quantum-secure Internet of Things (IoT) blockchain that emphasizes the use of PQC in securing distributed IoT networks against quantum attackers. Though their potential is high, these works are still theoretical and have not been applied much to real-life city use, such as smart parking^[15].

The comparison summary of existing research with the proposed work is shown below in Table 1. In this table, we demonstrate the novelty of the proposed framework and how we can address the limitations of the existing research studies with the help of the proposed framework.

Key considerations

The current literature highlights substantial progress in blockchain-based and IoT-enabled smart parking systems; nevertheless, substantial deficiencies persist regarding quantum resilience, end-to-end security, and automated trust enforcement. Most current solutions emphasize decentralization and openness, but they don't address new quantum

Table 1. Summary of comparison with existing research studies.

Research study	Technology	Quantum-resilience	Automated penalties	Immutable audit trail	Access control	Scalability	Computational overhead	Implementation status	Performance evaluation	Application domain
Ankarboina et al. ^[9]	ECC, AES-GCM, and JWT	×	×	×	JWT tokens	Moderate	Low	Prototype	Throughput and registration delay	Smart parking
Singh et al. ^[10]	AI, blockchain	×	×	✓	Mobile App	Moderate	Medium	Prototype	Slot allocation accuracy	Smart parking
Zhang et al. ^[11]	IoT, blockchain, SC	×	✓	✓	RFID/NFC	Moderate	Medium	Prototype	Transaction automation	Smart parking
Vijayalakshmi et al. ^[12]	Intrusion detection system	×	×	×	VANET	Moderate	High	Prototype	97% attack detection accuracy	Car parking system
Alymani et al. ^[13]	IoT, machine learning	×	×	×	Not specified	High	Medium	Prototype	Vehicle detection accuracy	Smart cities
Liu et al. ^[15]	PQC, blockchain	✓	×	✓	Not specified	Moderate	High	Research prototype	Security analysis	General IoT
Nanwatkar et al. ^[16]	IoT, AI, ML, Sensors	×	×	×	Mobile/web App	High	Medium	Prototype	Smart parking automation	Smart parking
Aslam et al. ^[5]	Quantum-resistant blockchain	✓	✓	✓	Blockchain contracts	Moderate	High	Prototype	Blockchain performance	Intelligent transportation
Proposed work	PQC, blockchain, SC, QR	✓	✓	✓	QR code	High	Moderate (15% over RSA)	Fully implemented prototype	Encryption time, blockchain latency, gas cost, QR validation time, end-to-end performance	Smart parking

RFID, Radio Frequency Identification; NFC, Near Field Communication.

threats or secure access validation methods. To solve these problems, this work suggests a single framework that combines PQC, blockchain technology, and QR-based access control into one end-to-end architecture. PQC-based encryption keeps sensitive user and transaction data safe from quantum attacks, and Ethereum-based smart contracts^[17] make it possible for financial transactions to be automated, open, and tamper-proof. Also, adding QR-code-based validation makes real-time access control stronger by connecting physical entrance and exit events with changes in the blockchain state^[18,19]. The proposed system is different from other systems because it offers a complete solution that meets the needs for privacy, openness, and automation in smart parking conditions all at once. Combining PQC with blockchain not only protects against future quantum threats but also makes the system stronger against regular cyberattacks. The framework's implementation and testing on a testnet show that it can be used in real-world smart city projects.

These are the essential requirements of the proposed framework:

- **Quantum-resilient security:** The proposed framework must guarantee security against both classical and quantum attacks through the implementation of post-quantum cryptography for secure and private data encryption and key exchange^[20–22].
- **Secure and automated transactions:** Smart contracts must facilitate automatic reservations, payment processing, penalty enforcement, and refunds with minimal human involvement.
- **Smart parking data privacy and integrity:** Confidential user and transaction information and smart parking data must be securely kept and safeguarded through encryption and authentication protocols^[23].
- **Decentralized trust and transparency:** The integration of blockchain is essential for establishing immutable, tamper-proof audit trails and eradicating dependence on centralized authorities.
- **Efficient access control mechanism:** A dependable QR code-based validation system and digital signature^[24–26] must be established to safely regulate vehicle ingress and egress, while deterring fraud and unauthorized access^[27].
- **Interoperability and integration:** The framework must facilitate easy integration with cloud services, IoT devices, and current smart city infrastructure^[28–32].
- **A decentralized post-quantum trust framework for secure IoT-enabled smart parking networks.**

Decentralized post-quantum trust framework for secure IoT-enabled smart parking networks

In this section, we discuss the post-quantum cryptography-based blockchain framework for smart parking, with an overview of the framework and mathematical flow, step by step. The proposed framework is structured as a multi-layered system, where each layer represents a specific module responsible for a particular function, with secure interaction among all layers. The frontend handles user registration, authentication, parking reservation, and QR codes. The backend handles booking requests, cryptographic operations, and communication with the blockchain network. Before booking data is stored, the PQC module takes care of its protection, with Ethereum smart contracts being responsible for the automation of the booking, payment, refund, and penalty processes. Lastly, QR-code validation securely synchronizes the physical access of vehicles with the

records in blockchain transactions, providing secure and transparent parking management.

Overview of framework

The proposed Framework is a combination of a strong set of PQC, Blockchain, and smart contracts that are suggested to solve the new security issue of smart parking systems, in particular, during the quantum era. In its simplest form, the architecture applies lattice-based PQC (Kyber KEM) to quantum-resistant key exchange and AES-GCM to effectively encrypt sensitive booking and user data, using AES-GCM and ensuring data integrity using SPHINCS+ digital signatures. MySQL is used as secure storage, and Firebase is used to provide user authentication, which guarantees both scalability and operational stability. Unchanging audit trails. It is possible to create immutable audit trails by writing all the reservation and payment events to an Ethereum blockchain, and using smart contracts, the financial transactions and penalties are automated and transparent.

The system also improves operational efficiency by using QR code-based access control, which directly associates physical entry and exit validation with blockchain state changes, which prevents fraud and provides uninterrupted user experiences. Experimental analyses show that the framework provides quantum-resilient confidentiality, transparent and tamper-proof auditing, and automated execution of penalties with moderate performance overhead compared to classical cryptography and centralized systems. The proposed architecture bridges PQC, blockchain, and real-time IoT validation in a single installation and creates a future-proof architecture of secure, decentralized, and smart parking infrastructures in smart cities. The overall architecture of the proposed VishwasQ framework is shown in Fig. 1, where the components involved in the front end, back end, cryptographic modules, blockchain infrastructure, and IoT parking validation are depicted.

The entire process starts with user authentication and parking space reservation via the web interface. The reservation information is encrypted using the proposed hybrid PQC scheme and safely stored in the database. At the same time, the Ethereum blockchain handles the transactions of booking and payments as smart contracts. Once the payment is confirmed, a QR code will be created for parking. The QR code is checked at entry and exit on the blockchain, providing secure access control and preventing unauthorized entry of vehicles.

Algorithmic workflow and protocol

We use a hybrid solution, which allows classical TLS (Transport Layer Security) compatibility with endpoints and uses PQC to protect stored data and session-sensitive payloads, providing quantum-resistant security, as mentioned in Algorithm 1. We combine a lattice-based KEM (Kyber), AES-GCM (symmetric encryption), and SPHINCS (digital signatures) to ensure integrity in our scheme. The general workflow comprises key generation, encapsulation, data encryption, storage, and secure decryption.

Algorithm workflow

- **Key Initialization:** The system initializes a long-term PQC key pair (pk, sk) for server-side operations.

- **Ephemeral Key Derivation:** For each user transaction, an ephemeral symmetric key k is derived via Kyber KEM encapsulation:

$$(ct, k) \leftarrow \text{Kyber.Encaps}(pk_{\text{server}}) \quad (1)$$

- **Data Encryption:** The user's sensitive booking data m is encrypted with AES-GCM using k :

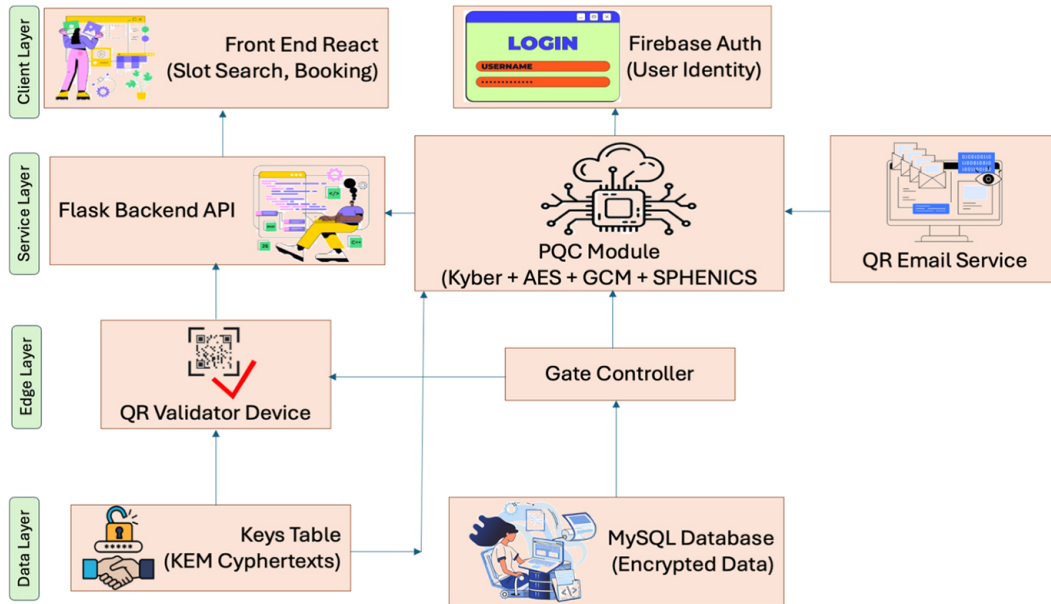


Fig. 1 A high-level overview of the proposed VishwasQ framework that depicts the relationship between the client layer and the service, edge, and data layers. The architecture features the development of user services using React, integration with Firebase for authentication, use of post-quantum cryptography (Kyber, AES-GCM, and SPHINCS+) for security, secure storage in MySQL, integration with the Ethereum blockchain and smart contracts, and QR code validation for parking accessibility.

Algorithm 1. PQC-based encryption protocol for a smart parking system.

Input: user booking data message, service public and private keys, and signature key pairs are the input for the PQC-based encryption protocol

m : User booking data message

pk_{server} : Server public key

sk_{server} : Server private key

(pk_{sig}, sk_{sig}) : Signature key pairs

Output: encrypted data tuple, decrypted message after successful verification is used as an output of the algorithm. ($msgid, c, ct, \sigma$): Encrypted data tuple

m : Decrypted message after successful verification

procedure

```

1: ENCRYPTDATA (message  $m, pk_{server}$ )
2:    $(ct, k) \leftarrow \text{Kyber.Encaps}(pk_{server})$ 
3:    $c \leftarrow \text{AES GCM.Encrypt}(k, m)$ 
4:    $\sigma \leftarrow \text{SPHINCS} + .\text{Sign}(sk_{sig}, c || ct)$ 
5:    $\text{DB.store}(msgid, c, ct, \sigma)$ 
6:   return( $msgid, c, ct, \sigma$ )

```

end procedure

procedure

```

7: DECRYPTDATA ( $msgid, sk_{server}$ )
8:    $(c, ct, \sigma) \leftarrow \text{DB.fetch}(msgid)$ 
9:    $k \leftarrow \text{Kyber.Decaps}(sk_{server}, ct)$ 
10:   $m \leftarrow \text{AES GCM.Decrypt}(k, c)$ 
11:  Verify  $\sigma$  with  $pk_{sig}$ 
12:  if verification succeeds, then
13:    return  $m$ 
14:  else
15:    return Failure
16:  end if

```

end procedure

$$c \leftarrow \text{AES - GCM.Enc}(k, m) \quad (2)$$

• **Data Storage:** The encrypted data c and KEM ciphertext ct are stored in the database, indexed by a unique message identifier $msgid$.

• **Signature Generation:** To ensure authenticity, a SPHINCS+ signature σ is generated:

$$\sigma \leftarrow \text{SPHINCS} + .\text{Sign}(sk_{sig}, c || ct). \quad (3)$$

• **Decryption:** During retrieval, the server decapsulates ct to recover k :

$$k \leftarrow \text{Kyber.Decaps}(sk_{server}, ct). \quad (4)$$

The data is then decrypted:

$$m \leftarrow \text{AES - GCM.Dec}(k, c). \quad (5)$$

• **Verification:** Finally, the SPHINCS+ signature σ is verified to ensure data integrity.

The secure cryptographic workflow of the proposed framework is shown in Algorithm 1. The session key is created using key encapsulation from Kyber, and the booking information is encrypted using AES-GCM, providing confidentiality and integrity of the data. The integrity of the stored data is then protected against classical and quantum attacks through the use of SPHINCS+ digital signatures when it is retrieved.

Smart contract design

Smart contracts are implemented on the Ethereum testnet to make or cancel a booking, provide an escrow for a payment, manage a session, and automatically impose a penalty. The contract also gets rid of intermediaries and makes financial transactions transparent and tamper-proof. Some of the main functions and their duties are as follows:

• **createReservation($msgid, slot, price$):** Locks the base fee into escrow and sets the session state to Reserved. Preconditions: The user is required to have enough money, and the slot has to be free. Postconditions: The booking entry with a unique identifier, which is the $msgid$.

• *startSession(msgid)*: Invoked by the validator device at entry. Logs the start time and changes the state of the session to Active. Checks the validators, who can only be authorized to initiate this call.

• *endSession(msgid)*: Invoked when the user exits. Records time out, actual time parked, and final charge calculated. In case of over-stay by the user, the deduction of penalty ties occurs automatically to the escrow before the rest of the money is released.

• *withdraw()*: Owner-only function to withdraw accumulated balances after penalty settlements. Ensures clear management of revenues.

Booking and payment workflow

The following Algorithm 2 shows the QR code validation process, and Algorithm 3 represents the Smart Contract parking workflow.

The proposed methodology combines authentication, quantum-resistant encryption, blockchain-based transaction management, and QR code validation in a single process. Parking events are meticulously documented on the blockchain, and the smart contracts ensure a seamless reservation, payment, and penalty system without the need for intermediaries. The integration not only enhances transparency but also minimizes manual processes and bolsters the overall security of the smart parking system.

The smart contract provides several security measures:

• Checks-effects-interactions pattern: Before any external calls are made, the internal state is updated, and this prevents reentrancy attacks.

Algorithm 2. QR code validation protocol (simplified).

Input: Identity of the user, QR code identifier, server private key used as input for QR code verification data.

user: Identity of the user

QRid: QR code identifier

sk_{server}: Server private key

Output: Success/failure status

Parking session state updated

procedure

```

1: VALIDATEQR(user, QRid)
2: booking ← DB.fetch(QRid)
3: data ← PQC.Decrypt(skserver, booking.encData)
4: if data.valid = True then
5:   if Session.state = "Entry" then
6:     SmartContract.updateState(QRid, Active)
7:     Gate.open()
8:     return Success
9:   else if Session.state = "Exit" then
10:    Tparked ← currentTime – data.startTime
11:    if Tparked > data.allowedTime then
12:      Penalty ← (Tparked – data.allowedTime) × Prate
13:      SmartContract.deduct(Penalty)
14:    else
15:      SmartContract.refund(user)
16:    end if
17:    SmartContract.updateState(QRid, Ended)
18:    Gate.open()
19:    return Success
20:  end if
21: else
22:    return Failure
23: end if
end procedure

```

• Access control: Validator addresses can only be used to make *startSession*, and only the owner may withdraw money. With the help of access control, no one can access the records without permission. If we have a user ID and password, then we can access the records; otherwise, we cannot access the records, it is part of Start Session.

• Reentrancy guards: According to the situation of the proposed system architecture, this is an essential task for Reentrancy Guards. These are implemented in sensitive functions to prevent recursive exploitation.

• Immutable state: According to the blockchain's features, when data is stored in the ledger, we cannot alter the data; it is called the Immutable or Tamper-Proof Ledger State. So, once finalized, session

Algorithm 3. Smart contract parking workflow.

Input: Message identifier, parking slot, and user's account are used as input to the smart contract parking workflow

msgid: Message identifier

slot: Parking slot

price: Parking price

user: User's account

Output: Reserved/Active/Ended: parking session state

Penalty/Refund: payment settlement

procedure

```

1: CREATERESERVATION(msgid, slot, price)
2: require(slot.available = True)
3: escrow[msgid] ← price
4: state[msgid] ← Reserved
5: emitEvent(ParkingReserved, msgid, slot, price)
end procedure
procedure
6: STARTSESSION(msgid)
7: require(state[msgid] = Reserved)
8: startTime[msgid] ← block.timestamp
9: state[msgid] ← Active
10: emitEvent(ParkingStarted, msgid, startTime[msgid])
end procedure
procedure
11: ENDESESSION(msgid)
12: require(state[msgid] = Active)
13: parkedTime ← block.timestamp – startTime[msgid]
14: if parkedTime > allowedTime[msgid] then
15:   overtime ← parkedTime – allowedTime[msgid]
16:   penalty ← overtime × penaltyRate
17:   escrow[msgid] ← escrow[msgid] – penalty
18:   transfer(penalty, owner)
19: end if
20: refund ← escrow[msgid]
21: transfer(refund, user[msgid])
22: state[msgid] ← Ended
23: emitEvent(ParkingEnded, msgid, parkedTime, penalty)
end procedure
procedure
24: WITHDRAW
25: require(msg.sender = owner)
26: transfer(contractBalance, owner)
end procedure

```

states are irreversible and thus can be audited. Smart parking records data is stored in the blockchain ledger as a tamper-proof or immutable state.

Gas and performance analysis: Ethereum test-net experiment deployment suggests the following average gas amounts:

- *createReservation()*: 65,000 gases
- *startSession()*: 5,000 gases
- *endSession()*: 80,000 gases (depends on the calculation of the penalty)
- *withdraw()*: 30,000 gases

Such costs are not high considering the small frequency of the parking transactions with respect to the high-frequency financial systems.

The entire end-to-end process of the post-quantum cryptography (PQC)-based secure smart parking system^[33], which starts with user booking and moves through payment, checking the parking availability, and closing the session, is depicted in Fig. 2. The process begins with the reservation of a parking spot by a user, and the sensitive booking information is encrypted by a hybrid PQC and AES-GCM method and stored safely in the backend database. Once at the parking facility, a validation of the QR code is carried out, which connects real-life input or output processes with the state changes in the blockchain, thereby guaranteeing access management and authenticity of transactions. Ethereum blockchain smart contracts^[34] automatically process payment settlements, overstay fines, and have tamper-resistant audit trails, so every activity of the parking process is securely and transparently recorded without human intervention. The entire operational process of the proposed framework, from parking reservation to blockchain payment settlement and QR code-assisted exit process, is shown in Fig. 2.

Implementation details

The execution of the suggested smart parking framework is based on the hybrid technology stack to provide not only quantum-resilient security but also operational efficiency. The framework was executed on a workstation running Windows 11 and an Intel Core i7

processor with 16 GB of RAM. React 18 and Firebase Authentication are used to create the frontend of the system to enable scalable and secure access by its users, whereas Python 3.11 with the liboqs-python/Open Quantum Safe (OQS) library, Flask, and PyMySQL are used to create a robust API (Application Programming Interface) service and database management. Quantum-resistant encryption is implemented using a library implementation of the Kyber-768 key encapsulation mechanism (corresponding to NIST Security Level 3) (KEM) and AES-256-GCM to encrypt sensitive booking data with a symmetric key. The encrypted payloads, keys, and signature artefacts are organized in a MySQL database, and the corresponding tables are used to store users, encrypted bookings, and cryptographic keys, which provide a rational data structure. The technology stack and functional components of the proposed quantum-resilient trust framework are shown in Table 2.

Its integration facilitates a decentralized audit trail, and in order to automate the reservations, payments, and punishments. Solidity-based smart contracts run on the Ethereum testnet (i.e., Sepolia or Goerli) are deployed. Parking facilities are controlled with physical access via a lightweight validator service on edge hardware (e.g., Raspberry Pi), which performs verification of QR codes. This staged implementation shows how the framework can integrate post-quantum cryptographic protection, automated financial transactions, and real-time access control, and deliver on system security and usability for smart city mobility solutions.

The reason for choosing Ethereum is its well-established smart contract ecosystem, security, large developer community, and stable Sepolia test network, which facilitated the implementation of the prototype and reproducible experimental evaluation. While some layer-2 solutions like Optimism, Arbitrum, and Polygon offer reduced transaction fees and lower latency, the major aim of this work is to attest to the viability of combining post-quantum cryptography with blockchain-based smart parking. As a result, Ethereum was used for the current prototype, and layer-2 and permissioned blockchain platforms are deemed to be potential avenues for future large-scale deployments.

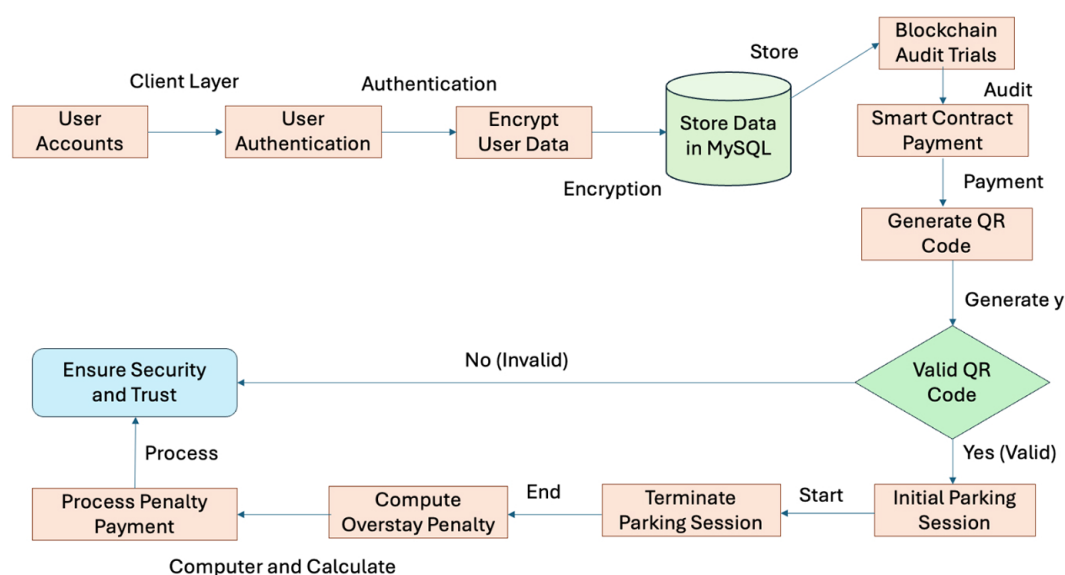


Fig. 2 Operational workflow of the proposed system starting from user authentication, parking reservation, data encryption with PQC, secure storage of data in the database, secure payment using blockchain, generation of QR and validation, parking session management, automated enforcement of penalties, and audit logging in the blockchain.

Table 2. Technology stack and functional components of the proposed quantum-resilient trust framework.

Layer/module	Technology/tools	Functionality	Description
Frontend layer	React 18, Firebase authentication	User interface and secure access	Provides a scalable and responsive UI for slot search, booking, and QR display with secure user authentication and session management
Backend service layer	Python 3.11, Flask, PyMySQL	API and business logic	Handles booking requests, slot allocation, payment initiation, and communication between frontend and database
PQC security module	Kyber-like KEM, AES-GCM	Quantum-resistant encryption	Implements hybrid encryption where Kyber secures symmetric keys and AES-GCM encrypts sensitive booking data, ensuring confidentiality and integrity
Database layer	MySQL	Data storage and management	Stores encrypted user data, booking information, cryptographic keys, and signature artifacts in structured tables
Blockchain layer	Ethereum testnet (Sepolia/Goerli), Solidity	Decentralized audit and smart contracts	Enables immutable audit trails and automates booking, payment, and penalty enforcement using smart contracts
Edge layer	Raspberry Pi (or similar IoT device)	QR code validation and access control	Performs real-time QR verification and controls physical gate access for parking entry/exit
QR code module	QR generator and validator	Secure access mechanism	Generates time-bound QR codes for booking validation and prevents unauthorized access
Payment and penalty module	Smart contracts (Solidity)	Automated transactions	Handles booking payments and penalty enforcement transparently and automatically via blockchain
System integration	Hybrid architecture	End-to-end system coordination	Integrates PQC, blockchain, backend, and IoT components to ensure secure, efficient, and real-time smart parking operations

Performance evaluation and analysis

This section demonstrates the performance and evaluation analysis of the proposed framework and shows the novelty through a comparison of the proposed work and existing research studies. We consider the suggested framework on three levels: (i) speed of encryption in a post-quantum and classic environment, (ii) blockchain transaction latency, and (iii) final booking latency, which was observed on the prototype system. Performance summary (Prototype) is shown in Table 3.

(i) Encryption performance: To evaluate the cryptographic overhead, we conducted a comparative analysis between a hybrid post-quantum scheme (Kyber KEM combined with AES-GCM) and a classical cryptographic approach (RSA-2048 with AES-GCM). The experimental results from our prototype implementation reveal that the PQC-based scheme introduces a modest increase in computational cost. This is primarily due to the nature of lattice-based arithmetic operations used in Kyber, which are inherently more CPU-intensive than the highly optimized modular arithmetic employed in RSA-based key encapsulation.

In quantitative terms, the hybrid PQC scheme incurs an approximate 15% increase in latency during booking-related encryption operations when compared to the RSA baseline. However, this additional delay remains within acceptable limits for practical deployment. Given the enhanced security guarantees offered by post-quantum cryptography, the observed overhead is a reasonable trade-off. Importantly, the latency remains well within the tolerable bounds of server-side processing for smart parking systems, ensuring that overall system performance and user experience are not adversely affected.

(ii) Blockchain latency: We evaluated blockchain confirmation delays through deployments on the Ethereum test network, where the average transaction confirmation time was observed to be approximately 15 s. This latency is primarily influenced by factors such as network congestion and the selected gas price. To support

near real-time validation, the proposed system integrates QR code-based entry verification with a backend validation mechanism. While the initial verification is handled instantly at the application layer, the blockchain layer ensures final settlement, providing tamper-proof records and immutable audit trails. This hybrid approach effectively balances responsiveness with the security and transparency guarantees of blockchain technology.

The prototype demonstrated 100% transaction execution success and steady throughput under the workload tested. Only the meta-data for transactions is kept on-chain, keeping storage costs low, and encrypted booking data is kept off-chain. The volume of gas used is slightly dependent on the execution of the smart contracts, and the congestion of the network primarily influences the confirmation time for transactions but not the accuracy of the system.

(iii) End-to-end booking latency: We further assessed user-perceived latency by measuring the time elapsed from the initiation of the booking process to the successful delivery of a valid QR code to the user. This end-to-end duration captures multiple critical operations, including post-quantum cryptographic (PQC) encapsulation, AES-GCM-based secure encryption, blockchain transaction submission, and email delivery. Despite the involvement of these computational and communication steps, the prototype achieved a median latency of approximately 2–4 s. This response time is well within acceptable limits for real-world urban parking scenarios, ensuring that users experience a smooth and responsive interaction. Overall, the system effectively maintains strong security guarantees without compromising usability, thereby delivering a practical and user-friendly solution.

Thread model and security analysis

The suggested framework is tested against a set of adversarial threats, such as eavesdropping, man-in-the-middle (MITM) attacks, database breaches, smart contract exploits, replay attacks, and quantum-enabled attackers.

Threat model

We suppose that attackers can seek to:

- Hack communication between users and the backend servers to retrieve sensitive booking data.
- Initiate TLS attacks to use session payloads using MITM.
- Hack the back-end database to steal stored user data and reservations.

Table 3. Performance summary (standard metrics).

Metric	Baseline (RSA)	Proposed (PQC + AES)
Key encapsulation time (ms)	18	21
Booking encryption overhead	0	15%
QR gen + email (ms)	1,500	1,700
Blockchain confirmation (s)	10–30	10–30

- Abuse Ethereum smart contract vulnerabilities (e.g., reentrancy, unchecked integer operations).
- Enter the old QR code or reservation ID and reply to gain unauthorized access.
- Make quantum computing break classical cryptography like RSA or ECC.

Defenses

The system combines several mechanisms to deal with these threats:

Protection against quantum attacks on privacy

Post-quantum cryptographic key encapsulation mechanisms, such as Kyber, play a crucial role in safeguarding sensitive data against emerging quantum threats. By securing the exchange of symmetric keys, Kyber ensures that confidential information and private communications remain protected even in the presence of powerful quantum adversaries. Unlike traditional cryptographic methods that may become vulnerable with the advent of quantum computing, Kyber is designed to withstand such attacks, thereby providing long-term security and future-proof protection for critical data.

Integrity and auditability

Storing booking events on the blockchain ensures the creation of a transparent and tamper-proof record of all system activities. Each reservation, payment transaction, and state change is securely logged in an immutable ledger, making it virtually impossible to alter or delete records. This not only enhances trust and accountability but also provides a reliable audit trail for verification and dispute resolution. As a result, stakeholders can confidently rely on the integrity of the data, knowing that every action within the system is permanently and securely recorded.

Smart contract security

The smart contract is carefully designed following well-established security best practices to minimize potential vulnerabilities. It adheres to the checks-effects-interactions pattern, ensuring that all validations and state updates are performed before any external interactions take place. Additionally, the inclusion of reentrancy guards helps prevent common attack vectors such as reentrancy attacks, which have historically led to significant exploits. The contract also restricts unsafe or unauthorized upgrades, preserving the integrity of its logic over time. Together, these measures create a robust and secure execution environment, making it considerably more difficult for attackers to exploit the system.

Operational security

Authentication of parking validator devices is implemented through a combination of mutual TLS (Transport Layer Security) and digital signature-based message verification. This dual-layer approach ensures that both the client and server verify each other's

identities before any communication takes place, establishing a trusted connection. In addition, every message exchanged is cryptographically signed and validated, guaranteeing its authenticity and integrity. As a result, the system effectively prevents device spoofing, unauthorized access, and other malicious activities, thereby strengthening the overall security of the parking infrastructure. The security analysis of the proposed VishwasQ framework against the common classical and quantum attack models and defense mechanisms incorporated in the system is shown in [Table 4](#).

The results show that the proposed framework counters major security threats by using post-quantum cryptography, blockchain, secure authentication, and smart contract technology in combination. These mechanisms jointly enhance confidentiality, integrity, authentication, and resilience to classical and quantum attacks.

Limitations

While the proposed framework significantly enhances security and resilience, it is not without certain limitations. One of the primary concerns is the computational overhead introduced by PQC, which is inherently more resource-intensive than traditional cryptographic techniques. This increased cost stems from complex mathematical operations, and it necessitates careful optimization through hardware acceleration and the use of highly efficient cryptographic libraries to ensure practical deployment. In addition, the reliance on blockchain introduces its own set of challenges. Transaction confirmation times can vary due to network latency, and gas fees are often unpredictable, which may impact the overall cost and responsiveness of the system. To address these issues in real-world deployments, alternative approaches such as layer-2 scaling solutions or permissioned blockchain networks can be adopted to improve performance, reduce latency, and provide more consistent operational costs.

Evaluation discussion

When post-quantum cryptography and blockchain work together, they find a balance between quantum-resistant privacy and trust that is distributed. The proposed framework can be implemented in the smart parking domain, where secure payments, transparent audit trails, and automated enforcement are also significant points of concern, because it can be instantiated with only a small overhead on performance. The proposed architecture is compared to the traditional parking system in [Fig. 3](#) to illustrate its benefits in terms of security, transparency, and automation. Nevertheless, the production systems of the future should pay attention to the elements of gas costs on the public blockchain, the user experience of on-chain payments, legal aspects of cryptocurrency use, and the scalability of validator infrastructure.

[Figure 4](#) shows the experimental performance evaluation of the proposed framework in terms of scalability and cryptographic overhead. [Figure 4a](#) shows how the total number of users affects system

Table 4. Security analysis of the proposed VishwasQ framework.

Attack type	Security mechanism	Mitigation
Replay attack	QR code with time limit and blockchain verification of transactions	Stops reuse of expired or duplicate transactions
MITM attack	Kyber-KEM, AES-256-GCM, TLS-authentication	Offers private and authenticated conversations
Sybil attack	Identity verification with blockchain and Firebase authentication	Prevents creation of fake identities without permission
Denial-of-service (DoS)	Smart contract verification and backend request validation	Reduces malicious handling of requests and unauthorized access
Smart contract attack	Checks-Effects-Interactions pattern along with re-entrancy guard	Prevents re-entry and unauthorized contract execution
Database tampering	AES-GCM encryption and unalterable blockchain audit logs	Protects confidentiality and integrity of data at rest
Quantum attack	Kyber KEM and SPHINCS+	Resists quantum adversaries

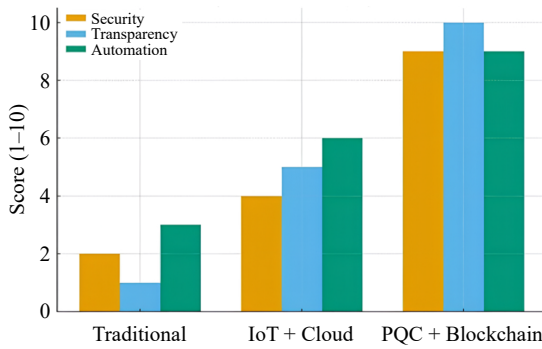


Fig. 3 Traditional, IoT-cloud-based, and the proposed PQC-blockchain parking system are compared qualitatively regarding security, transparency, and automation. The proposed framework combines the quantum resistance of cryptography with decentralized blockchain services to achieve the best overall performance.

latency. The increase we see is mostly because of delays in blockchain confirmations and the extra work that cryptography requires. Even so, the latency is still within an acceptable range for smart parking apps that work in real time. Figure 4b shows that the PQC-based encryption scheme adds a small amount of overhead when compared with classical RSA-based encryption. But this trade-off makes the system quantum-resistant, which means it will be safe from future cryptographic threats.

The comparison in Table 5 shows that IoT-only systems^[30] have weak security and a lack of trust because they are controlled from

one central location. On the other hand, blockchain-based systems make data more transparent and trustworthy, but they are still open to quantum attacks. The suggested system combines post-quantum cryptography using blockchain and QR-based validation to improve security standards, automated procedures, and tamper-proof auditing. It does add some extra processing and latency, but it strikes a good balance between speed, scalability, and security that will last. Because of this, the proposed design is better for parking systems in smart cities of the future.

Conclusions

This paper introduced a decentralized post-quantum trust framework for secure IoT-enabled smart parking networks that incorporates PQC-based confidentiality encryption in the form of a blockchain, which allows auditability to be immutable, and smart contracts that automate payments and penalties on Ethereum. A working prototype can be used to prove the practicality of the architecture, where quantum-resistant confidentiality and decentralized trust are possible with reasonable performance trade-offs. The suggested system is highly transparent, automatable, and security-friendly in the post-quantum world by improving the future of urban parking. The proposed framework will be improved with regard to scalability, efficiency, and intelligence in the future to facilitate large-scale deployments in smart cities. Although it is promising in its performance, the proposed framework has its set of limitations that can be addressed in future research. Post-quantum

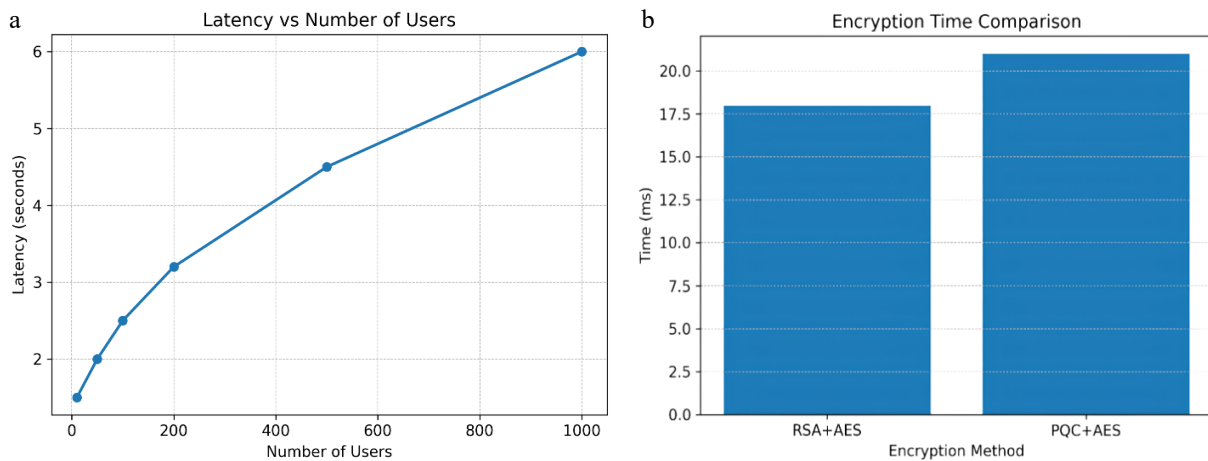


Fig. 4 Assessment of the proposed framework. Scalability characteristics of the framework. (a) System latency vs number of concurrent users. In (b), the execution time of the proposed PQC-AES scheme is compared with the conventional RSA-AES method, showing that the computational overhead of PQC is modest.

Table 5. Smart parking framework/architecture comparative analysis.

Parameter	IoT-only system	Blockchain-based system	Proposed approach (PQC + blockchain + QR)
Security-level	Low (classical encryption)	Medium (blockchain integrity)	High (PQC + blockchain security)
Quantum resistance ^[35]	No	No	Yes
Data integrity	Vulnerable to tampering	Immutable records	Immutable + cryptographically secure
Privacy protection	Limited	Moderate	Strong (PQC encryption)
Access control	RFID/sensors	Smart contract-based	QR code + blockchain validation
Automation of payments	Manual/semi-automatic	Automated via smart contracts	Fully automated with penalty enforcement
Transparency	Low	High	Very high
Scalability	High	Moderate (gas cost issues)	Moderate (optimizable with layer 2)
Latency	Low	High (blockchain delay)	Moderate (optimized hybrid flow)
Suitability for smart cities ^[36,37]	Limited	Good	Excellent

cryptography (PQC) integration may introduce some computational overhead compared to traditional cryptographic algorithms, and during extensive implementations, the time required to confirm blockchain transactions and gas fees could impact the responsiveness of the system. In addition, the current implementation has been tested on a prototype environment using the Ethereum test network and has not yet been tested in a real-world smart city scenario with a high number of concurrent users and a multitude of different IoT devices.

Future efforts will involve enhancing the framework's scalability and efficiency by implementing hardware-accelerated versions of PQC algorithms, exploring the potential of adopting Layer-2 blockchain or permissioned blockchain solutions to lower latency and transaction costs, and introducing formal verification of smart contracts to further reinforce the security of the system. The framework will also be expanded to accommodate the interoperability of the system with intelligent transportation systems and other smart city infrastructure. Additionally, the use of AI for demand forecasting, flexible parking assignment, and dynamic price models will be explored, further optimizing the use of resources and improving the experience for users in future smart mobility applications.

These future improvements will enhance the scalability, security, and practical applicability of the presented framework, enabling its integration into next-generation intelligent transport systems and quantum-resistant smart city environments. Finally, the developed VishwasQ framework offers a practical and scalable approach for secure smart parking systems, providing quantum-resilient security, transparent transaction management, and automated trust mechanisms that support the deployment of next-generation smart city and intelligent transportation infrastructures.

Author contributions

The authors confirm their contributions to the paper as follows: conceptualization, methodology, software/implementation: Patadiya A, Savaliya U, Jadav Y; validation: Suthar OP; writing – original draft: Patadiya A, Savaliya U, Jadav Y; writing – review and editing: Suthar OP, Singh SK, Lee HL; supervision: Singh SK. All authors reviewed the results and approved the final version of the manuscript.

Data availability

This study does not use publicly available datasets. All relevant data supporting the findings are included within the manuscript.

Acknowledgments

The authors would like to thank the Department of Computer Engineering at Marwadi University for their continuous support. We also acknowledge the open-source PQC and blockchain communities for providing algorithms, tools, and libraries that enabled the successful implementation of this prototype.

Conflict of interest

The authors declare that they have no conflict of interest.

Dates

Received 19 June 2026; Revised 14 July 2026; Accepted 10 September 2026; Published online 30 September 2026

References

- Reddy KS, Sowjanya P. 2026. An improved ECC-based authenticated key exchange protocol for industrial IoT environments. *International Journal of Communication Systems* 39(5):e70438
- Shah AM, Gor A. 2025. Comprehensive survey of symmetric and public-key cryptographic algorithms: foundations, attacks, and applications. *International Journal of Informative and Futuristic Research* 12(10):20–38
- Alatawi MN. 2025. Blockchain-driven smart contracts for advanced authorization and authentication in cloud security. *Electronics* 14(15):3104
- Almutairi M, Sheldon FT. 2025. IoT–cloud integration security: a survey of challenges, solutions, and directions. *Electronics* 14(7):1394
- Aslam AM, Bhardwaj A, Chaudhary R. 2025. Quantum-resilient blockchain-enabled secure communication framework for connected autonomous vehicles using post-quantum cryptography. *Vehicular Communications* 52:100880
- NIST. 2022. *Post-Quantum cryptography standardization*. <https://csrc.nist.gov/Projects/post-quantum-cryptography>
- Bos J, Ducas L, Kiltz E, Lepoint T, Lyubashevsky V, et al. 2018. CRYSTALS - kyber: a CCA-secure module-lattice-based KEM. *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, London, UK, 2018. London, UK: IEEE. pp. 353–367 doi: 10.1109/eurosp.2018.00032
- Bernstein DJ, Buchmann J, Dahmen E. 2009. *Post-Quantum Cryptography*. Berlin, Heidelberg: Springer. doi: 10.1007/978-3-540-88702-7
- Ankarboina H, Kumari J, Chandan Kumar P, Ananth AD, Bhardwaj A, et al. 2026. A secure lightweight and queue-balanced smart parking architecture for vehicular networks: design, analysis, and evaluation. *Results in Engineering* 30:110334
- Singh SK, Pan Y, Park JH. 2022. Blockchain-enabled secure framework for energy-efficient smart parking in sustainable city environment. *Sustainable Cities and Society* 76:103364
- Zhang C, Zhu L, Xu C, Zhang C, Sharif K, et al. 2020. BSFP: blockchain-enabled smart parking with fairness, reliability and privacy protection. *IEEE Transactions on Vehicular Technology* 69(6):6578–6591
- Vijayalakshmi S, Bose S, Logeswari G, Maheswaran N. 2025. Smart parking: intelligent intrusion detection system in VANET enabled car parking system. *Automatika* 66(2):281–299
- Alymani M, Almoqhem LA, Alabdulwahab DA, Alghamdi AA, Alshahrani H, et al. 2025. Enabling smart parking for smart cities using Internet of Things (IoT) and machine learning. *PeerJ Computer Science* 11:e2544
- Parida NK, Jatoth C, Reddy VD, Hussain MM, Faizi J. 2023. Post-quantum distributed ledger technology: a systematic survey. *Scientific Reports* 13:20729
- Liu A, Zhang Q, Xu S, Feng H, Chen XB, et al. 2024. QBIOT: a quantum blockchain framework for IoT with an improved proof-of-authority consensus algorithm and a public-key quantum signature. *Computers, Materials & Continua* 80(1):1727–1751
- Nanwatkar R, Dome V. 2025. A comprehensive review of smart parking systems: technologies, challenges, and future directions. *International Journal of Manufacturing and Materials Processing* 11(1):1–13
- Atzei N, Bartoletti M, Cimoli T. 2017. A survey of attacks on ethereum smart contracts (SoK). In *Proceedings of the 6th International Conference on Principles of Security and Trust*. Volume 10204. Berlin, Heidelberg: Springer. pp. 164–186 doi: 10.1007/978-3-662-54455-6_8
- Ibrahim M, Lee Y, Kahng HK, Kim S, Kim DH. 2022. Blockchain-based parking sharing service for smart city development. *Computers and Electrical Engineering* 103:108267
- Yang Z, Alfauri H, Farkiani B, Jain R, Di Pietro R, et al. 2024. A survey and comparison of post-quantum and quantum blockchains. *IEEE Communications Surveys & Tutorials* 26(2):967–1002
- Almuhammadi S, Alghamdi S. 2025. A novel transition protocol to post-quantum cryptocurrency blockchains. *Frontiers in Computer Science* 7:1457000

- [21] Castiglione A, Esposito JG, Loia V, Nappi M, Pero C, et al. 2025. Integrating post-quantum cryptography and blockchain to secure low-cost IoT devices. *IEEE Transactions on Industrial Informatics* 21(2):1674–1683
- [22] Wicaksana A. 2025. A survey on quantum-safe blockchain security infrastructure. *Computer Science Review* 57:100752
- [23] Akash S, Mary Joans S, Mukunthrajan T, Karthikeyan P. 2024. Smart parking management system using AI enhanced by quantum network. In *Quantum Networks and Their Applications in AI*, eds Ananth C, Khalaf OI, Anand J. USA: IGI Global. pp. 321–336 doi: [10.4018/979-8-3693-5832-0.ch020](https://doi.org/10.4018/979-8-3693-5832-0.ch020)
- [24] Kim K, Choi S, Kwon H, Kim H, Liu Z, et al. 2020. PAGE—practical AES-GCM encryption for low-end microcontrollers. *Applied Sciences* 10(9):3131
- [25] Deshpande S, Lee Y, Karakuzu C, Szefer J, Paek Y. 2025. SPHINCSLET: an area-efficient accelerator for the full SPHINCS⁺ digital signature algorithm. *ACM Transactions on Embedded Computing Systems* 24(5):1–19
- [26] Fadavi M, Azimi SA, Karati S, Jaques S. 2025. DGSP: An efficient scalable fully dynamic group signature scheme using SPHINCS⁺. Cryptology ePrint Archive. Paper 2025/760 <https://eprint.iacr.org/2025/760>
- [27] Huang PC, Chang CC, Li YH, Liu Y. 2018. Efficient access control system based on aesthetic QR code. *Personal and Ubiquitous Computing* 22(1):81–91
- [28] Lee S, Kim JH. 2024. Opportunistic block validation for IoT blockchain networks. *IEEE Internet of Things Journal* 11(1):666–676
- [29] Singh CP, Yamaganti R, Umrao LS. 2025. A privacy-preserving and secure framework using blockchain-based quantum-inspired complex convolutional neural network for IoT-driven smart cities. *Peer-to-Peer Networking and Applications* 19(1):3
- [30] Ahmad AYAB, Verma N, Sarhan NM, Awwad EM, Arora A, et al. 2024. An IoT and blockchain-based secure and transparent supply chain management framework in smart cities using optimal queue model. *IEEE Access* 12:51752–51771
- [31] Padma A, Ramaiah M. 2024. Blockchain based an efficient and secure privacy preserved framework for smart cities. *IEEE Access* 12:21985–22002
- [32] Wang Y, Shahril Ismail E. 2025. A review on the advances, applications, and future prospects of post-quantum cryptography in blockchain and IoT. *IEEE Access* 13:112962–112977
- [33] Mansoor K, Afzal M, Iqbal W, Abbas Y. 2024. Securing the future: exploring post-quantum cryptography for authentication and user privacy in IoT devices. *Cluster Computing* 28(2):93
- [34] Crisostomo J, Bacao F, Lobo V. 2025. Machine learning methods for detecting smart contracts vulnerabilities within Ethereum blockchain – a review. *Expert Systems with Applications* 268:126353
- [35] Singh H, Bari S, Singh SK, Suthar OP. 2025. AI-driven predictive analytics for secure IoT-enabled smart agriculture and public administration perspectives. In *Transforming Public Administration Through AI-Driven Predictive Analytics*, eds Kumar P, Hamid AA, Nand P, Kumar R. USA: IGI Global Scientific Publishing. pp. 49–94 doi: [10.4018/979-8-3373-3760-9.ch002](https://doi.org/10.4018/979-8-3373-3760-9.ch002)
- [36] Prajapati Y, Suthar OP, Gosai K, Singh SK. 2025. Smart city cybersecurity: leveraging machine learning for advanced ransomware detection and prevention. *2025 International Conference on Pervasive Computational Technologies (ICPCT)*, Greater Noida, India, 2025. Greater Noida, India: IEEE. pp. 808–813 doi: [10.1109/ICPCT64145.2025.10941048](https://doi.org/10.1109/ICPCT64145.2025.10941048)
- [37] Suthar OP, Vaghela K, Katkar V, Prajapati Y, Khan H. 2025. Anomaly detection in 6G smart cities using machine learning and deep learning. *Security Paradigms in 6G Smart Cities and IoT Ecosystems*. Boca Raton: CRC Press. pp. 140–156 doi: [10.1201/9781003564645-11](https://doi.org/10.1201/9781003564645-11)



Copyright: © 2026 by the author(s). Published by Maximum Academic Press, Fayetteville, GA. This article is an open access article distributed under Creative Commons Attribution License (CC BY 4.0), visit <https://creativecommons.org/licenses/by/4.0/>.