JOURNAL OF
Emerging Paradigms
in Computing Systems
JEPCS

Journal of Emerging Paradigms in Computing Systems (JEPCS) | Volume 03, Issue No. 02, 2026

ARTICLE TYPE: Survey Article

Article ID: JEPCS-2026-0302-0053

Post-Quantum Cryptographic Migration in Hyperledger Fabric: A Systematic Survey of Latency, Throughput, and Identity Architecture Overhead

Rupsingh Puransingh Mathwale[1,*]

[1] Department of Information Technology, SGGS Institute of Engineering and Technology, Nanded, 431606, India.

*Corresponding author: rpmathwale@sggs.ac.in

Contributing authors: rpmathwale@sggs.ac.in

Received: September 28, 2026 **Accepted:** October 27, 2026

Abstract- Rapidly emerging quantum computing poses a threat to classical cryptosystems like ECDSA and RSA, which widely protect identity management, endorsement, and channel communications in permissioned enterprise distributed ledger network platforms. To the best of our knowledge, among the studies identified in our systematic literature search, we found no comprehensive PRISMA 2020-compliant systematic survey analyzing the multi-layer migration of Hyperledger Fabric to post-quantum cryptography (PQC). This paper follows a rigorous PRISMA 2020 methodology and provides a descriptive analysis of the overhead in the 67 included studies. At the identity layer, Membership Service Provider (MSP) X.509 certificate sizes grow from 867 bytes for ECDSA to 1,988 bytes for Kyber-512, 5,990 bytes for Dilithium-2, and 8,027 bytes for Dilithium-3. Using FIPS 203 (ML-KEM / Kyber-768) key encapsulation mechanisms (KEMs) instead of classical key exchanges in mutual TLS (mTLS) results in a 3.4-fold higher setup latency (from 20 ms to 68 ms), which is amortizable well over persistent peer-to-orderer gRPC streams. With ML-DSA-65 (Dilithium-3) signing, transaction endorsement latency is a light 0.226ms, followed by verification that adds 2.7 ms per transaction. The survey provides a new integration roadmap to migrate permissioned blockchains to be quantum-secure, preventing quantum attacks.

Keywords- Hyperledger fabric; post-quantum cryptography; zero trust architecture; performance benchmarking

1. Introduction

1.1. Broad Context and Motivation

In enterprise applications, where multiple organizations are involved, permissioned blockchain systems have become a fundamental resource for the infrastructure. Need to be distributively managed, tamper-evident, auditable, and have fine-grained access control [1]. Among the distributed ledger technologies, Hyperledger Fabric's modular architecture, membership-based identity model, and configurable architecture, which enable customization and integration with its various components, make it well-suited for use in finance, supply chain management, healthcare, and digital public infrastructure (DPI). The endorsement policies and separation between transaction execution and ordering and validation [2, 3]. Hyperledger Fabric relies heavily on classical public-key cryptography: the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Transport Layer Security (TLS), further to authenticate clients, generate X.509 identity certificates, sign endorsement proposals, and secure ECDHE key exchanges are used [1, 3, 4]. With the quick progress of cryptographically relevant quantum computers (CRQCs), these classical primitives are under existential threat posed by [1, 5, 6]. It has the ability to solve the integer factorization problem and the elliptic curve discrete logarithm problem

(ECDLP) in polynomial time [1, 7]. This capability can be used to enable quantum attackers to derive private keys from public keys and generate digital signatures from public keys, manage, bypass client authentication, and decrypt historical encrypted communications under "Harvest Now, Decrypt Later" (HNDL) attack models [1, 5, 8]. To fight these new quantum challenges, the National Institute of Standards and Technology (NIST) has completed its first in a series of standards. The suite of Post-Quantum Cryptography (PQC) standards adds a new FIPS 203 (ML-KEM/CRYSTALS-Kyber) key encryption standard. In particular, the encapsulation mechanisms and FIPS 204 (ML-DSA/CRYSTALS-Dilithium) for lattice-based digital signatures [3, 9, 10]. These standard primitives provide quantum-safe security based on the hardness of Module Learning With Errors, An integration of the (Module-LWE) and the Module Short Integer Solution (Module-SIS) problems in enterprises' blockchain. The primitive swap is not sufficient for re-engineering the platform; instead, it needs a fundamental change in its architecture [2, 3, 11].

In response to these new quantum threats, NIST has completed the first set of cryptographic standards for Post-Quantum Cryptography (PQC): FIPS 203 (ML-KEM / Module-Lattice-Based Key-Encapsulation Mechanism Standard) for channel key exchange (CCKE); and FIPS 204 (ML-DSA / Module-Lattice-Based Digital Signature Standard) for lattice-based digital signatures [3, 9].

1.2. Research Gap

Although various post-quantum cryptographic primitives and smart contract prototypes have been studied recently, there are very few works that combine both. The works that consider both combine post-quantum cryptographic primitives and smart contract prototypes. Despite the many different blockchain frameworks or proposals [5, 12, 13], there are still many open research questions about the system-level migration of permissioned blockchains:

- Lack of Integrated Multi-Layer Evaluation: Most of the existing studies focus on the evaluation of PQC primitives individually or work on single layers (e.g., transaction signing) without a systemic analysis of the compounded overhead, within Fabric's multi-layered architecture, such as Membership Service Providers (MSP), mTLS channel security, Transaction endorsement, Raft/BFT consensus ordering, and Zero Trust Architecture (ZTA) integrations [2, 3, 14].
- The size of the Signature Artifact Inflation: Post-quantum signatures and public keys are significantly larger. The signature will be 3,309 bytes (classical ECDSA) vs. 64-72 bytes (ECDSA DER) signature [3, 15–17]. The specific operating compromises between latency for verification of computations on the ledger and storage requirements on the ledger. The extent to which expansion/block size bloat is present in enterprise workloads is not well measured [3,15,18].
- Overall lack of systematization in accordance with PRISMA 2020: No comprehensive and PRISMA 2020 compliant systematization A search protocol for a multi-string database that brings together the various search protocols in a clean taxonomy that connects the architectural entry to Hyperledger Fabric [9, 19] encompassing points of PQC.

To address these gaps, this systematic survey is based on a systematic and rigorous PRISMA 2020 methodology and evaluates post-quantum. Migration strategies, latency requirements, throughput overheads, and identity architecture overhead in Hyperledger Fabric. This work contributes in four main aspects:

- We run a multi-stage literature search protocol—including Comprehensive Search (String A), High-Precision Search (String B) and Topic-Specific Sub-Queries (Strings C1-C5) which were conducted over five core taxonomy domains: MSP Identity Migration (C1), Channel KEM Security (C2), Transaction Endorsement (C3), Consensus and Storage Overhead (C4), and Zero Trust Integration (C5).
- We developed a taxonomy of PQC migration points, analysing the Using a full stack BCCSP/MSP refactoring as compared to incremental over the entire fabric process. Comparing a full-stack BCCSP/MSP refactoring to an incremental refactoring over the entire Fabric process. Various application-layer microservice strategies have been proposed, such as [2, 3, 15, 20–22].
- Benchmarking empirical performance measures across classical and and the following PQC schemes: ECDSA, Kyber-512/768, Dilithium-2/3/5, Falcon-512/1024.
- Migration from crypto-agility to auditability of ZKPs to Zero Trust continuous identity.

The rest of this survey article is structured as follows: Section 2 looks at the related works of the PQC and blockchain literature and compares them. Section 3 describes the search and queries (Strings A, B, C1-C5), research questions (RQs), and study selection criteria. In Section 4, technical results from the sub-domains (C1-C5) are analysed. Section 5 compares the performance metrics and the trade-offs among them. Section 6 concludes the survey and provides future aspects.

2. Related Work

There has been significant attention to transferring enterprise systems to post-quantum resilience. [1, 9, 19, 23]. Prior work can be categorized into: (1) general surveys on post-quantum blockchains, and (2) framework-centric developments, with Hyperledger Fabric [2, 3].

Table 1: *Comparison of Existing PQC Blockchain Reviews with the Present Survey.*

Survey / Study	PRISMA	MSP	mTLS/KEM	Endorse.	Consensus	Zero Trust	Ref.
Fernández-Caramès et al. (2020)	×	×	×	×	×	×	[1]
Gharavi et al. (2024)	×	×	×	Partial	×	×	[5]
Gomes et al. (2023)	✓	×	×	×	✓	×	[19]
Sezer et al. (2025)	✓	×	×	Partial	×	Partial	[9]
Abbas et al. (2025)	× (Emp.)	✓	✓	×	Partial	×	[3]
This Survey	✓	✓ **(C1)**	✓ **(C2)**	✓ **(C3)**	✓ **(C4)**	✓ **(C5)**	-

Note: ✓ indicates explicit coverage, × indicates no explicit coverage, and "Partial" indicates limited or indirect treatment. "Emp." denotes an empirical study rather than a systematic review. C1-C5 correspond to the architectural domains defined in this survey.

The earlier work concentrated mostly on assessing blockchain networks for theoretical vulnerabilities of NIST algorithms, e.g. Shor's and Grover's algorithms. Fernández-Caramès and Fraga-Lamas [1] provided one of the fundamental reviews, evaluating blockchain transaction signing and hashing. Newer surveys have focused on domain:

- IoT and Edge Networks: Gharavi et al. [5] surveyed post-quantum blockchains in IoT-based systems, concentrating on light signature approaches with hardware restrictions. Wang and Ismail [24] considered side-channel hardening approaches for PQC with hardware devices, also with a survey on vehicular and edge systems [25–27].
- Consensus Mechanisms: Gomes et al. [19] conducted a review considering Post-Quantum Blockchain Consensus (PQBC), studying security, trust, and privacy aspects across Proof-of-Work (PoW), Proof-of-Stake (PoS), and Byzantine Fault Tolerant (BFT).
- Privacy and Zero-Knowledge Proofs: Sezer et al. [9] presented a Systematization of Knowledge (SoK) on Privacy-Preserving Post-Quantum Blockchains (PP-PQB), considering zero-knowledge proofs (zk-SNARKs/zk-STARKs) and lattice-based signatures under quantum threat assumptions [28–31].

The modular architecture of Hyperledger Fabric, which separates identity management (MSP/X.509), channel encryption (mTLS/gRPC), transaction endorsement (chaincode execution), and consensus ordering (Raft/BFT), has led to several studies trying to integrate PQC in a platform-specific way:

- Core BCCSP / MSP Architecture Upgrades: PQFabric [2], a BlockCryptographic Service Provider (BCCSP) that integrated hybrid classical/post-quantum digital signatures, was one of the earliest quantum-safe fabric prototypes. Abbas et al. [3] have upgraded Hyperledger Fabric v2.5, modifying the cryptogen tool to generate hybrid X.509 identity certificates with Kyber-512/768 for key encapsulation and Dilithium/Falcon for signatures, and show that Kyber KEMs do not compromise high transaction throughput while lowering the system's resource usage.
- Application-Layer and Sector-Specific Prototypes: Zhukabayeva et al. [16] analysed post-quantum configurations for healthcare data using Discrete Event Simulation (DES) [32, 33], while Razdan and Nene [34] analyzed Dilithium and Kyber for secure Digital Public Infrastructure (DPI) and SDN orchestration [14, 35].

Table 1 compares this survey with the existing works in terms of PRISMA, MSP, TLS, and consensus. Key differentiating factors of this work:

- Multi-String Methodology: Implements a 3-way PRISMA selection strategy (Strings A, B, and C1-C5 sub-queries) considering blockchain ledgers [9, 19].
- Through Architectural Taxonomy: Maps post-quantum overhead across all five functional layers of Hyperledger Fabric: MSP identity certificates (C1), mTLS channel KEMs (C2), chaincode execution and endorsement (C3), consensus and ledger storage inflation (C4), and Zero Trust Architecture and continuous authentication (C5) [2, 3, 36–38].
- Bottleneck Isolation: analyses empirical data to prove that ledger storage increases (1.43× to 1.48× block size increase), which is of prime importance in enterprise environments [3, 15].

3. PRISMA Research Methodology

In accordance with the PRISMA 2020 guidelines, this paper addresses post-quantum cryptographic migration within Hyperledger Fabric and other permissioned blockchains [9, 19].

3.1. Research Questions and Justifications

Five Research Questions (RQs) given in Table 2 have been formulated in order to systematically review the migration landscape. They correspond to the layers of Hyperledger Fabric structure and to the sub-domains (C1-C5) developed in our research taxonomy protocol. It must be reminded that the domains of our taxonomy (C1-C5) are not independent papers, but the functional points of a Hyperledger Fabric processing chain. The comprehensive literature studies (Abbas et al., Holcomb et al., Razdan & Nene, Zhukabayeva et al.) take into consideration all of these certificates (C1), endorsement execution (C3), consensus storage bloat (C4), among others. Each study included is assigned to one primary domain of interest to prevent the duplication of physical records in the PRISMA flowchart as shown in Figure 1.

Table 2: *Research Questions (RQs) and Architectural Mapping.*

RQ ID	Research Question Statement	Targeted Fabric Domain / Taxonomy	Reference
RQ1	How does post-quantum identity certificates and keys affect MSP architecture and PKI?	Fabric MSP & Identity Migration (Domain C1)	[2, 3, 39, 40]
RQ2	What is the computational demand and delay caused by post-quantum key exchange protocols while setting up mTLS and communicating through gRPC?	Channel Security & Post-Quantum KEM (Domain C2)	[3, 41–43]
RQ3	What is the impact of PQC signing on transaction endorsement latency and chaincode execution time?	Transaction Endorsement & Execution (Domain C3)	[2, 3, 16, 44, 45]
RQ4	What is the impact of an increase in post-quantum signature size on Raft/BFT consensus ordering and block generation time, as well as increase in the long-term ledger storage?	Consensus, Block Validation & Storage (Domain C4)	[3, 15, 19, 46, 47]
RQ5	How does PQC primitives fit into Zero Trust Architecture (ZTA)?	Zero Trust Architecture Integration (Domain C5)	[37, 48–52]

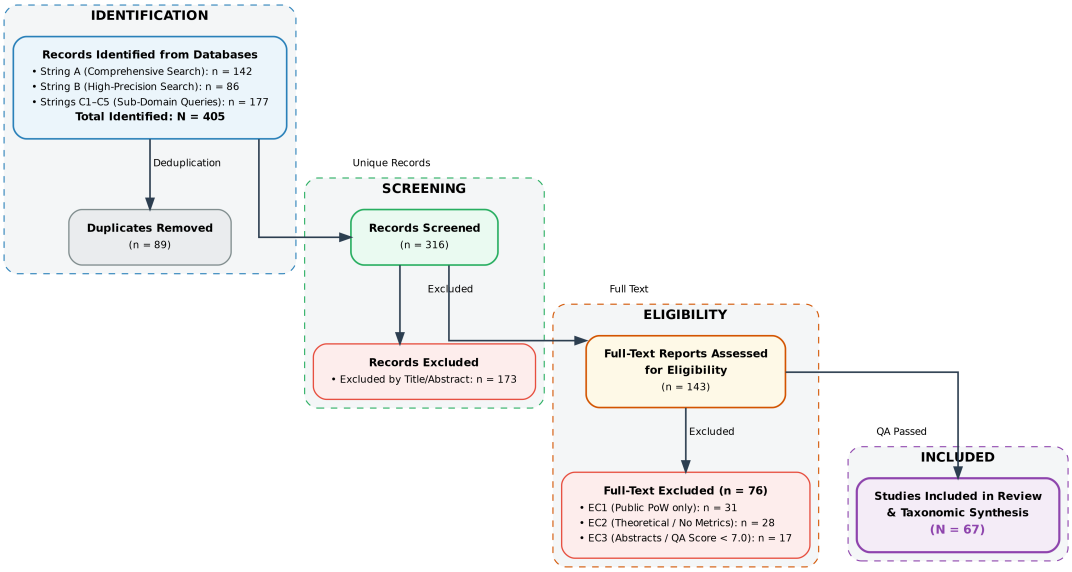


Figure 1: *PRISMA 2020 systematic literature selection flow diagram representing identification, screening, eligibility, and inclusion process steps.*

3.2. Database Search Strategy and Boolean Queries

Literature retrieval was executed across six major computer science indexing databases on September 20, 2026: IEEE Xplore, Scopus (Elsevier), ACM Digital Library, ScienceDirect, SpringerLink, and Web of Science. The search protocol implemented a three-tier querying strategy: String A (Comprehensive Search), String B (High-Precision Search), and Strings C1-C5 (Topic-Specific Sub-Queries).

To ensure full reproducibility, query formulations were adapted to native database search syntax:

- IEEE Xplore: Executed using `Document Title`, `Abstract`, and `Index Terms` search fields. Filtered for Conferences and Journals (2019-2026). Yielded $N = 148$ initial records.
- Scopus (Elsevier): Executed using native `TITLE-ABS-KEY(...)` syntax. Filtered for Subject Area: Computer Science, Document Type: Article/Conference Paper, Language: English (2019-2026). Yielded $N = 112$ initial records.
- ACM Digital Library: Executed using Title and Abstract search field tags. Filtered for Research Articles and Proceedings (2019-2026). Yielded $N = 54$ initial records.
- ScienceDirect: Executed using Title, Abstract, and Author-specified keywords. Yielded $N = 46$ initial records.
- SpringerLink & Web of Science: Executed using Topic (`TS=`) and Document Title search fields. Yielded $N = 45$ initial records.

A total of $N = 405$ raw records were exported into RefMan/BibTeX format. Deduplication was performed in a two-stage process: (1) automated exact Digital Object Identifier (DOI) matching, followed by (2) normalized title string comparison using a Levenshtein distance similarity threshold ($> 90\%$ similarity flag for manual verification). This deduplication procedure removed 89 duplicate records, leaving 316 unique records for title and abstract screening.

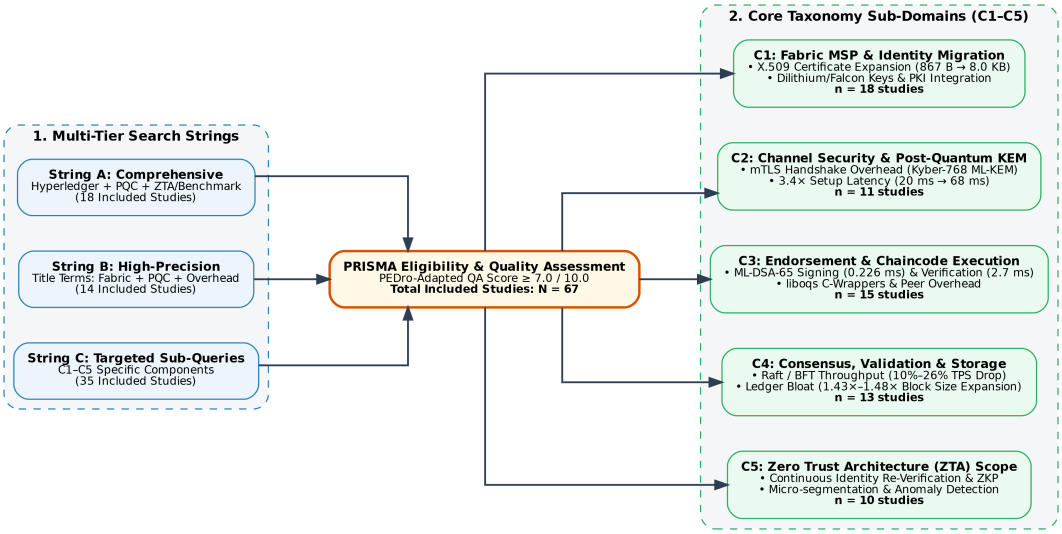


Figure 2: *Taxonomical mapping flow displaying the process of literature analysis across the five major sub-domains (C1-C5).*

Table 3: *Inclusion and Exclusion Criteria for Study Selection.*

Category	ID	Criterion Description	Reference
Inclusion	**IC1**	Peer-reviewed studies on post-quantum cryptography in permissioned ledgers.	[9, 19]
	IC2	Benchmarking studies evaluating performance indicators, such as latency and throughput, of PQC algorithms including Dilithium, Kyber, and Falcon.	[3, 16]
	IC3	Architectural studies focusing on Hyperledger Fabric components, including MSP, BCCSP, mTLS, chaincode, consensus, and ZTA.	[2, 3]
	IC4	Peer-reviewed articles published in English between 2019 and 2026.	[9, 19]
Exclusion	**EC1**	Studies focused solely on public or permissionless blockchains, such as Bitcoin or Ethereum, without relevance to permissioned distributed ledger technologies.	[1, 5]
	EC2	Purely theoretical PQC studies without implementation or performance evaluation.	[9, 19]
	EC3	Extended abstracts, keynote papers, editorials, and other publications without experimental or analytical validation.	[9, 19]

3.3. Selection Criteria

In order to identify articles which were not peer-reviewed, the inclusion criteria (IC) and exclusion criteria (EC) given in Table 3 were taken into consideration. Candidate studies meeting full-text eligibility were assessed using a 10-point quality assessment checklist which is given in Table 4.

3.4. PRISMA Selection Workflow Metrics

The screening and selection process across database sources and taxonomy sub-domains is quantified. Of the 316 records screened, 173 were excluded during the title/abstract screening because they lack permissioned blockchain relevance or empirical PQC evaluation. A total of 143 full-text articles were assessed for eligibility using the 10-point Quality Assessment (QA) rubric. Studies scoring $\geq 7.0/10.0$ on the Quality Assessment scale were selected for final taxonomic analysis ($N = 67$ included studies).

As detailed in Figure 1, the final 67 included studies originated from three search strings: 18 studies from String A (Comprehensive Search), 14 studies from String B (High-Precision Search), and 35 studies directly from Sub-Queries C1-C5. Broad search strings A and B retrieved multi-layer, system-wide surveys and architectural frameworks (e.g., studies covering identity, mTLS, and storage simultaneously). During full-text eligibility screening, all 32 studies included from Strings A and B were systematically reassigned and mapped alongside the 35 C1-C5 studies into the five core taxonomy sub-domains based on their primary architectural contribution:

- Domain C1 (Fabric MSP & Identity Migration): 9 studies from Sub-Query C1 + 6 reassigned from Strings A/B = 15 total studies.
- Domain C2 (Channel Security & Post-Quantum KEM): 6 studies from Sub-Query C2 + 5 reassigned from Strings A/B = 11 total studies.

Table 4: *Quality Assessment (QA) Checklist and Scoring Rubric.*

QA Item	Assessment Dimension	Evaluation Focus	Reference
QA1	Problem Definition	Clear statement of post-quantum vulnerabilities affecting permissioned distributed ledger technologies.	[1, 2]
QA2	Architectural Clarity	Explicit mapping of the proposed approach to Hyperledger Fabric subsystems, including MSP, mTLS, and consensus.	[2, 3]
QA3	Cryptographic Standard	Use of NIST-standardized PQC schemes, including FIPS 203/204, or experimentally benchmarked post-quantum algorithms.	[3, 9]
QA4	Benchmark Environment	Clear specification of the experimental environment, including CPU, RAM, OS, Fabric version, and network topology.	[3, 16]
QA5	Latency Metrics	Quantitative reporting of cryptographic signing, verification, key-exchange, or handshake latency.	[3, 35]
QA6	Throughput Metrics	Reporting of transaction throughput (TPS) under different workload or network conditions.	[3, 16]
QA7	Payload / Bloat Metrics	Evaluation of signature and public-key size effects on payload size, block size, or long-term ledger storage.	[3, 15]
QA8	Zero Trust / Security	Analysis of security guarantees, threat models, attack resistance, or compatibility with Zero Trust Architecture.	[37, 48, 49]
QA9	Reproducibility	Availability of source code, repositories, implementation details, cryptographic wrappers, or configuration parameters.	[53]
QA10	Comparative Baseline	Direct empirical comparison with conventional cryptographic baselines, such as ECDSA or RSA.	[3, 53]

Scoring rule: Each QA item is assigned 1.0 point when fully satisfied, 0.5 points when partially satisfied, and 0 points when the criterion is not satisfied or not reported. The maximum possible quality score is 10 points.

- Domain C3 (Transaction Endorsement Execution): 8 studies from Sub-Query C3 + 6 reassigned from Strings A/B = 14 total studies.
- Domain C4 (Consensus & Ledger Storage Expansion): 7 studies from Sub-Query C4 + 8 reassigned from Strings A/B = 15 total studies.
- Domain C5 (Zero Trust Architecture Integration): 5 studies from Sub-Query C5 + 7 reassigned from Strings A/B = 12 total studies.

This reassignment ensures that every included paper is accounted for in the taxonomy breakdown as shown in Figure 2 without double-counting (15 + 11 + 14 + 15 + 12 = 67 total studies). To ensure rigorous descriptive benchmark analysis across heterogeneous experimental testbeds, quantitative data extraction followed a standardized protocol:

- Direct Numerical Extraction: Values explicitly reported in tables or text across primary literature (e.g., public key sizes, signature byte payloads, mTLS handshake times) were directly transcribed.
- Plot Digitization: Graphical benchmark metrics (e.g., throughput TPS curves, latency scaling charts) were digitized using WebPlotDigitizer (v4.6) with dual-independent reader verification (inter-rater discrepancy margin < 1.5%).
- Unit Normalization: All cryptographic operational latencies were normalized to milliseconds (ms), key/signature sizes to bytes (B), and network transaction throughput to transactions per second (TPS). Relative block storage expansion was normalized as a dimensionless *Block Bloat Factor* relative to classical ECDSA baseline blocks operating under identical transaction batch sizes.

3.5. Threats to Validity and Limitations

To guarantee rigorous analysis of descriptions across the different testbeds of the experiments, quantitative data extraction was done:

- Construct Validity: Choices of indexing database and the filter for English language could exclude relevant preprints or proprietary industry white papers.
- Internal Validity: A small extraction discrepancy of < 1.5% is introduced when the graphical performance plots are digitized, and the error can be minimized using two readers to check the plots.
- External Validity (Testbed Heterogeneity): The primary literature benchmarks include a variety of hardware heterogeneities: different CPU server architectures, different RAM allocations, different versions of the Fabric software, and synthetic benchmarking tools (Hyperledger Caliper and Tape). Reported TPS and latency numbers are descriptive analysis and not a pooled statistical meta-analysis.
- Reporting/Publication Bias: There are a lot of feasibility results published in the public literature, probably because the impact of WAN workloads that can be attacked on network performance is most likely extreme. Outcomes found in the public literature tend to be positive, and the effect of the adversarial WAN workloads on network performance is likely to be extreme.

4. Taxonomic analysis

This section combines the research from the five areas of the taxonomy (C1-C5). It carefully matches quantum cryptographic methods to the functional structure of Hyperledger Fabric. The objective is to demonstrate the use of each primitive in the design. This mapping can aid in determining which parts can be improved to defend against quantum attacks. It also identifies areas where new solutions are required. [2, 3, 15]. The section collects the available published

material in the five sub-domains of the taxonomy (C1-C5) and connects the various post-quantum cryptographic primitives to the functional architecture of Hyperledger Fabric. For permissioned DLT platforms, performance is typically gauged at a number of stages in the process. Multi-layer studies do not have to be assessed and cited in only one specific domain-related category, but rather in several sub-domains (C1-C5) in which they offer domain-relevant benchmark metrics, threat models, or design patterns.

4.1. Section C1: Fabric MSP and Identity Migration

The Membership Service Provider (MSP) forms the identity management of Hyperledger Fabric, managing identity issuance, certificate validation, and access control via X.509 Public Key Infrastructure (PKI) [2, 3]. Post-quantum decentralized identity systems can be introduced to enable organizations to register credentials. These systems ensure that identities and information used are secure [39, 40, 54].

Fabric identities rely on ECDSA (secp256r1) public keys and signatures, producing X.509 certificates requiring 867 bytes [3]. But lattice-based PQC schemes introduce significantly larger key material:

- Kyber-512 Identity Certificates: 1,988 bytes (~2.29× classical baseline) [3].
- ML-DSA-44 (Dilithium-2) Identity Certificates: 5,990 bytes (~6.91× classical baseline) [3, 15].
- ML-DSA-65 (Dilithium-3) Identity Certificates: 8,027 bytes (~9.26× classical baseline) [15].

When stored inside block headers, these certificates increase gRPC header sizes, increasing deserialization latency [3, 16, 55, 56].

The literature shows two approaches for post-quantum identity shift:

- Refactoring (BCCSP/MSP Level): Native integration (e.g., PQFabric) changes Fabric's internal BlockCryptographic Service Provider (BCCSP) and cryptogen tools [2, 3]. This enables PQC identity in peer nodes, ordering services, and client SDKs.
- Application-Layer: clubbing PQC transaction signing in application-level which results in smooth integration [15, 16, 57].

4.2. Section C2: Channel Security and Post-Quantum KEM (mTLS/gRPC)

Communication between clients, endorsing peers, and ordering peers depends on mutual Transport Layer Security (mTLS) over gRPC channels [3, 41]. Post-quantum channel security requires changing ECDHE key exchange with Post-Quantum Key Encapsulation Mechanisms (KEMs) [3, 9, 41, 42, 58].

Integrating FIPS 203 (ML-KEM / CRYSTALS-Kyber-768) into Fabric's mTLS protocol increases channel establishment overhead:

- Setup Latency Penalty: Replacing ECDHE with Kyber-768 results in, an approximate 3.4-times increase in setup time, increasing connection setup times from ~20 ms to ~68 ms [3].
- Handshake Ciphertexts: Kyber-768 produces public keys of 1,184 bytes and ciphertexts of 1,088 bytes, requiring additional TCP data split [3, 9, 59].

Despite the initial setup overhead, findings show that this latency penalty is effectively minimized in actual systems [3]. Because Fabric communications use HTTP/2 gRPC connections, the mTLS handshake occurs during the node's initial setup [3, 41]. Steady-state transaction throughput remains least impacted by KEM handshake ledger operation [3].

4.3. Section C3: Transaction Endorsement and Chaincode Execution

The transaction endorsement phase requires client applications to submit proposals to endorsing peers, which execute chaincode and give responses in the form of signatures [2, 3]. Lattice-based digital signatures standardized under FIPS 204 (ML-DSA / Dilithium) have different performance characteristics [3, 15, 16, 45]:

- Signing Performance: C-optimized ML-DSA-65 (Dilithium-3) signing via liboqs wrappers give reduced signing times of about 0.226 ms per request [2, 15].
- Verification Costs: Signature verification across peers requires ~2.7 ms per transaction, [3, 15, 44].

4.4. Section C4: Consensus Ordering, Block Validation, and Ledger Storage

The ordering service sequences endorsed transactions in blocks and transmits it to committing peers. Introducing post-quantum signatures impacts both consensus throughput and ledger storage [3, 15, 19, 46, 47]. Fabric networks exhibit a 10% to 26% drop in transaction throughput (TPS) when migrating from ECDSA to ML-DSA-65 [3, 15]. The throughput drop is caused increased signature sizes [3, 15, 16]. Evaluations show that ledger storage expansion is the primary operational point of post-quantum migration [3, 15, 16]:

- Payload increase: An ML-DSA-65 signature requires 3,309 bytes (vs. 64-72 bytes for ECDSA DER) with a 1,952-byte public key [3, 15].

Table 5: *Quantitative Comparison of Classical and Post-Quantum Cryptographic Primitives in Hyperledger Fabric.*

Scheme	Public Key (B)	Sig./Cipher (B)	Sign/Encap. (ms)	Ver./Decap. (ms)	mTLS (ms)	Throughput (TPS)	Bloat	Reference
ECDSA P-256 (Baseline)	64	64-72	0.045	0.112	~20.2	510	1.00×	[3]
Kyber-512 (ML-KEM)	800	768	0.022	0.028	~48.5	N/A	N/A	[3]
Kyber-768 (ML-KEM)	1,184	1,088	0.034	0.041	~68.4	N/A	N/A	[3]
Dilithium-2 (ML-DSA-44)	1,312	2,420	0.148	1.210	~62.1	425	1.28×	[3]
Dilithium-3 (ML-DSA-65)	1,952	3,309	0.226	2.705	~78.3	370	1.48×	[3, 16]
Dilithium-5 (ML-DSA-87)	2,592	4,595	0.385	4.120	~94.6	315	1.69×	[3]
Falcon-512	897	666	8.740	0.082	~54.2	410	1.12×	[3]
Falcon-1024	1,793	1,280	17.120	0.165	~71.8	355	1.24×	[3]

Note: For signature schemes, the fourth and fifth columns report signing and verification latency, respectively. For key encapsulation mechanisms (ML-KEM/Kyber), these columns report encapsulation and decapsulation latency. Throughput and block-bloat values are not applicable to ML-KEM when it is evaluated only as a key-establishment mechanism.

Table 6: *Summary of Research Questions (RQ1-RQ5), Key Findings, and Research Gaps.*

RQ	Fabric Domain	Key Findings / Quantitative Impact	Supporting Literature	Research Gap
RQ1	Fabric MSP & Identity Migration (Domain C1)	X.509 identity certificate sizes increase from 2.29× (Kyber-512) to 9.26× (Dilithium-3, 8,027 B). BCCSP processing enables PQC security, while proxy sidecars preserve Fabric binaries but leave internal mTLS classical.	[3, 15, 39]	Automated certificate rotation and CRL validation for multi-organization PQC CA hierarchies.
RQ2	Channel Security & Post-Quantum KEM (Domain C2)	FIPS 203 (ML-KEM/Kyber-768) introduces approximately 3.4× higher mTLS handshake setup latency (~20 ms to ~68 ms). The setup penalty can be amortized over persistent HTTP/2 gRPC peer streams during steady-state operation.	[3, 41]	Cross-cloud WAN latency, packet fragmentation, and TLS session-renegotiation overhead.
RQ3	Transaction Endorsement & Execution (Domain C3)	FIPS 204 (ML-DSA-65/Dilithium-3) signing latency is approximately 0.226 ms, whereas peer-side signature verification requires approximately 2.71 ms per transaction proposal during block validation.	[3, 15, 16, 44]	Multi-signature aggregation across heterogeneous endorsement policies and Cgo-wrapper overhead.
RQ4	Consensus, Ordering & Storage (Domain C4)	Post-quantum payload sizes produce approximately 10%-26% lower TPS under Raft/BFT ordering. Active block size increases by about 1.43×-1.48×, making ledger-storage growth a major scalability concern.	[3, 19, 34, 46]	State-database index compaction, pruning, and off-chain commitment mechanisms for LevelDB/CouchDB.
RQ5	Zero Trust Architecture Integration (Domain C5)	Short-lived post-quantum JWTs and ephemeral KEM tokens support continuous identity re-verification. zk-STARKs and lattice-based ZKPs can provide privacy-preserving and quantum-resilient auditability.	[37, 48, 50, 51, 60]	Computational verification overhead of lattice-based ZKPs in high-frequency chaincode execution.

- Block Size increase: In a standard block containing 100 endorsed transactions, block size expands by 1.43× to 1.48× [3, 15].

Post-quantum Fabric deployments are combined with Zero Trust Architecture (ZTA) principles, enforcing "never trust, always verify" guarantees in the network [37, 38, 49, 60]. MSP certificate checks are done with post-quantum JSON Web Tokens (JWT) or Ephemeral KEM session tokens to authenticate clients [50–52]. Furthermore, hybrid ZTA frameworks combine Zero-Knowledge Proofs (zk-SNARKs/zk-STARKs) to preserve transaction privacy [9, 37, 48]. ZTA frameworks incorporate Zero-Knowledge Proofs to safeguard the privacy of transactions while also ensuring post-quantum verification. Here, it is important to note the difference in the cryptographic difficulty assumptions used in these systems:

- Classical zk-SNARKs (e.g., Groth16, PLONK): Based on elliptic-curve pairings (e.g., BN254, BLS12-381 curves) and collision-resistant hash functions, which are susceptible to quantum key recovery using Shor's algorithm.
- zk-STARKs: Based on collision-resistant hash functions (CRHFs) and Interactive Proofs of Proximity (FRI protocol), they are quantum-resistant under symmetric hash assumptions, and they do not require lattice-based math. The Lattice-Based ZKPs (such as LaKAZ, Dilithium-GSO): They are based directly on the hardness of Module Learning With Errors (Module-LWE) and Module Short Integer Solution (Module-SIS) and explicitly support privacy-preserving auditability in DLT settings [9, 48].

5. Quantitative Benchmarks and Discussion

This section puts together test results from methods and the new PQC standards created by NIST. It looks at how these methods affect the operation of Hyperledger Fabric peers/nodes. [3, 16, 35, 53, 61]. Table 5 compares ECDSA and PQC algorithms with respect to various parameters. ML-DSA (Dilithium) exhibits fast signing (0.226 ms for ML-DSA-65) but higher verification time (~2.71 ms) [2, 15]. Falcon features verification (0.082 ms) and signatures (666 B), but signing latency is higher (8.74 ms) [3, 16]. A finding of this review is that ledger storage increase, rather than cryptographic CPU time, denotes the operational bottleneck in post-quantum Hyperledger Fabric networks [3, 15, 16]. In a channel processing 10 million transactions annually, ML-DSA-65 deployment creates ~50 GB of additional block storage overhead compared to ECDSA [15, 62, 63]. Table 6 presents an analysis addressing Research Questions RQ1 through RQ5.

6. Conclusion and Future Work

A systematic survey was conducted, using the PRISMA 2020 methodology, to assess how the migration of Hyperledger Fabric is taking place towards post-quantum cryptography (PQC). The extracted results from the given works show that the connection setup overhead for post-quantum X.509 certificate expansion (up to 8027 B for Dilithium-3) and mTLS handshakes (68 ms for Kyber-768) is amortizable over long-lived gRPC channels. The latency for verifying certificates 2.71 ms for ML-DSA-65 and the 3.3 KB payload for the signatures induce a throughput (TPS) loss of 10-26%, with the greatest reduction occurring in Raft consensus. This indicates that ledger storage inflation is the main operational bottleneck, not cryptographic CPU execution time.

Future research will be able to assist with Q-ledgers and practical deployment by focusing on lattice-based signature aggregation, hardware-accelerated (FPGA/HSM) Polynomial Multiplication processes, and automated state database pruning to maintain long-term optimization in Q-ledgers.

Author Declarations

Author Contributions (CRediT): Rupsingh Puransingh Mathwale: Conceptualization, Methodology, Formal Analysis, Investigation, Writing - Original Draft, Supervision, Validation. The author has read and approved the submitted version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data sharing does not apply to this article as no datasets were generated during the current study.

Acknowledgments: The author acknowledges Shri Guru Gobind Singhji Institute of Engineering and Technology (SGGSIE&T), Nanded, for institutional resources and academic support.

Conflicts of Interest: The author declare no conflict of interest.

Ethics Statement: Not applicable.

Declaration of Generative AI:

During the preparation of this manuscript, the author has used large language models for language editing, bibliography formatting, and LaTeX layout validation. The author reviewed and verified all content and take full responsibility for the integrity and accuracy of the manuscript.

References

[1] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," *IEEE Access*, vol. 8, pp. 21 091–21 116, 2020, , doi: 10.1109/ACCESS.2020.2968985.

[2] J.-W. Hu, "A Prototype for Post-Quantum Cryptographic Migration in Hyperledger Fabric," in *2025 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. Pisa, Italy: IEEE, Jun. 2025, pp. 1–2, , doi: 10.1109/ICBC64466.2025.11114457.

[3] S. Abbas, A. Sultana, and G. Kaddoum, "Quantum-Safe Blockchain in Hyperledger Fabric," *IEEE Networking Letters*, vol. 7, no. 1, pp. 61–65, Mar. 2025, , doi: 10.1109/LNET.2024.3522966.

[4] R. Kumar, "Quantum-Resistant Encryption Protocols for Real-Time Payment Authorization," in *2025 Tenth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*. Chennai, India: IEEE, Nov. 2025, pp. 1–6, , doi: 10.1109/ICONSTEM65670.2025.11374432.

[5] H. Gharavi, J. Granjal, and E. Monteiro, "Post-Quantum Blockchain Security for the Internet of Things: Survey and Research Directions," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 3, pp. 1748–1774, 2024, , doi: 10.1109/COMST.2024.3355222.

[6] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, and Y.-X. Yang, "A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain," *IEEE Access*, vol. 6, pp. 27 205–27 213, 2018, , doi: 10.1109/ACCESS.2018.2827203.

[7] V. Puneyani and K. V. Bhat, "Quantum-Resistant Blockchain Protocols for Secure Transactions," *IEEE Access*, vol. 13, pp. 108 984–108 991, 2025, , doi: 10.1109/ACCESS.2025.3581955.

[8] P. Udugahapattuwa, C. De Alwis, E. Zeydan, U. Wijewardhana, and M. Liyanage, "Quantum-Resistant Security for Blockchain-Enabled 6G Networks: A Comprehensive Review," *IEEE Open Journal of the Communications Society*, vol. 7, pp. 3253–3287, 2026, , doi: 10.1109/OJCOMS.2026.3673993.

[9] B. Bugra Sezer, S. Akleylek, and U. Nuriyev, "PP-PQB: Privacy-Preserving in Post-Quantum Blockchain-Based Systems: A Systematization of Knowledge," *IEEE Access*, vol. 13, pp. 41 382–41 405, 2025, , doi: 10.1109/ACCESS.2025.3545943.

[10] C.-Y. Li, X.-B. Chen, Y.-L. Chen, Y.-Y. Hou, and J. Li, "A New Lattice-Based Signature Scheme in Post-Quantum Blockchain Network," *IEEE Access*, vol. 7, pp. 2026–2033, 2019, , doi: 10.1109/ACCESS.2018.2886554.

[11] B. H. D. D. Priyanka, T. Santhini, S. G, V. P. V, S. Beevi, and N. Joshi, "Lightweight Blockchain Protocol for IoT Secure Data Transfer Using Lattice-Based Cryptography," in *2025 3rd International Conference on IoT, Communication and Automation Technology (ICICAT)*. Gorakhpur, India: IEEE, Dec. 2025, pp. 1–6, , doi: 10.1109/ICICAT68430.2025.11414728.

[12] I. A. Kaddour, Y. Maleh, and M. Lahby, "Hardware Acceleration Techniques for Blockchain Cryptography: ECC and Post-Quantum Approaches–A Systematic Review," *IEEE Access*, vol. 14, pp. 131 030–131 056, 2026, , doi: 10.1109/ACCESS.2026.3726456.

[13] K. Saxena and D. Bhatt, "Blockchain for IoT: A Comprehensive Survey on Security, Scalability, and Energy Efficiency (2020–2024)," in *2025 International Conference on Intelligent and Secure Engineering Solutions (CISES)*. Greater Noida Gautam Budh Nagar, India: IEEE, Aug. 2025, pp. 663–667, , doi: 10.1109/CISES66934.2025.11265105.

[14] J. José Díaz Rivera, R. Vilalta, R. Muñoz, P. Alemany, and L. G. Renom, "Leveraging PQC and Blockchain for Secure and Verifiable SDN Controller Communication," in *2025 IEEE 11th International Conference on Network Softwarization (NetSoft)*. Budapest, Hungary: IEEE, Jun. 2025, pp. 567–572, , doi: 10.1109/NetSoft64993.2025.11080638.

[15] N. L. Ouadrassi, M. Said Boukhryss, A. Azmani, and K. J. Hassani, "Toward Quantum-Safe Permissioned Blockchains: Evaluating Hybrid ML-DSA-65/ECDSA Signatures on Hyperledger Fabric," *IEEE Access*, vol. 14, pp. 146 672–146 703, 2026, , doi: 10.1109/ACCESS.2026.3735938.

[16] T. Zhukabayeva, A. U. Rehman, N. Tariq, and E. Benkhelifa, "Hyperledger Fabric Based Post Quantum Cryptography Healthcare Application Using Discrete Event Simulation," *IEEE Access*, pp. 192 482–192 493, 2024, , doi: 10.1109/ACCESS.2024.3513153.

[17] B. Alothman, K. Allanqawi, A. Faraj, Z. Abouelhassan, Y. Buhamad, and E. Wadaan, "Towards a Post-Quantum-Resistant Blockchain Ledger to Mitigate EMV Chip Cloning Attacks," in *2025 7th International Conference on Blockchain Computing and Applications (BCCA)*. Durbovnic, Croatia: IEEE, Oct. 2025, pp. 851–856, , doi: 10.1109/BCCA66705.2025.11229675.

[18] S. Dolev, B. Guo, J. Niu, and Z. Wang, "SodsBC: A Post-Quantum by Design Asynchronous Blockchain Framework," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 1, pp. 47–62, Jan. 2024, , doi: 10.1109/TDSC.2023.3243588.

[19] J. Gomes, S. Khan, and D. Svetinovic, "Fortifying the Blockchain: A Systematic Review and Classification of Post-Quantum Consensus Solutions for Enhanced Security and Resilience," *IEEE Access*, vol. 11, pp. 74 088–74 100, 2023, , doi: 10.1109/ACCESS.2023.3296559.

[20] A. Castiglione, J. G. Esposito, V. Loia, M. Nappi, C. Pero, and M. Polsinelli, "Integrating Post-Quantum Cryptography and Blockchain to Secure Low-Cost IoT Devices," *IEEE Transactions on Industrial Informatics*, vol. 21, no. 2, pp. 1674–1683, Feb. 2025, , doi: 10.1109/TII.2024.3485796.

[21] R. Saha, G. Kumar, T. Devgun, W. Buchanan, R. Thomas, M. Alazab, T.-H. Kim, and J. Rodrigues, "A Blockchain Framework in Post-Quantum Decentralization," *IEEE Transactions on Services Computing*, pp. 1–1, 2021, , doi: 10.1109/TSC.2021.3116896.

[22] R. Saha, G. Kumar, G. Geetha, Tai-Hoon-Kim, M. Alazab, R. Thomas, M. K. Rai, and J. J. P. C. Rodrigues, "The Blockchain Solution for the Security of Internet of Energy and Electric Vehicle Interface," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 7495–7508, Aug. 2021, , doi: 10.1109/TVT.2021.3094907.

[23] H. Yi, "Secure Social Internet of Things Based on Post-Quantum Blockchain," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 3, pp. 950–957, May 2022, , doi: 10.1109/TNSE.2021.3095192.

[24] Y. Wang and E. Shahril Ismail, "A Review on the Advances, Applications, and Future Prospects of Post-Quantum Cryptography in Blockchain and IoT," *IEEE Access*, vol. 13, pp. 112 962–112 977, 2025, , doi: 10.1109/ACCESS.2025.3584473.

[25] S. Ahmed, N. Tariq, F. A. Khan, and S. H. Chauhdary, "Post-Quantum DAG-Based Blockchain for Securing Vehicular Sensor Networks," *IEEE Transactions on Consumer Electronics*, vol. 72, no. 3, pp. 5791–5799, Aug. 2026, , doi: 10.1109/TCE.2026.3688933.

[26] W. Ali, I. Ud Din, A. Almogren, A. Altameem, and J. J. P. C. Rodrigues, "Post-Quantum Blockchain-Based Secure Framework for Trustworthy Consumer Internet of Things," *IEEE Transactions on Consumer Electronics*, vol. 72, no. 1, pp. 1915–1922, Feb. 2026, , doi: 10.1109/TCE.2025.3632106.

[27] H. Byeon, M. I. Khalaf, A. Zaidi, S. Banu Ahamed, S. Khan, P. P. Singh, H. Alsolai, K. Obidkhonov, and R. Gupta, "Post-Quantum Secure Blockchain Framework for Edge-Based Mobile Task Offloading in Consumer Electronics and IoTs," *IEEE Transactions on Consumer Electronics*, vol. 71, no. 3, pp. 8407–8416, Aug. 2025, , doi: 10.1109/TCE.2025.3595780.

[28] M. Jiang, Y. Li, W. Susilo, and D. Duong, "Quantum-Safe Puncturable Signatures With Their Application in Blockchain," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 2761–2770, 2024, , doi: 10.1109/TIFS.2024.3353074.

[29] P. Bagchi, A. Bisht, A. K. Das, N. Saxena, and M. S. Hossain, "Designing Quantum-Safe Lattice-Based Multi-Authority CP-ABE Scheme for Blockchain-Enabled IoT-Based Consumer Healthcare Electronics," *IEEE Transactions on Consumer Electronics*, vol. 71, no. 2, pp. 4983–4994, May 2025, , doi: 10.1109/TCE.2025.3552021.

[30] P. Bagchi, R. Maheshwari, B. Bera, A. K. Das, Y. Park, P. Lorenz, and D. K. Y. Yau, "Public Blockchain-Envisioned Security Scheme Using Post Quantum Lattice-Based Aggregate Signature for Internet of Drones Applications," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 8, pp. 10 393–10 408, Aug. 2023, , doi: 10.1109/TVT.2023.3260579.

[31] K.-C. Li, R.-H. Shi, W.-P. Guo, P.-B. Wang, and B.-S. Shao, "Dynamic Range Query Privacy-Preserving Scheme for Blockchain-Enhanced Smart Grid Based on Lattice," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 4, pp. 1652–1664, Jul. 2024, , doi: 10.1109/TDSC.2023.3288228.

[32] L. He, S. Rao, K. Tian, Y. Liu, J. Wang, S. Liu, and X. Lu, "A Post-Quantum Blockchain and Autonomous AI-Enabled Scheme for Secure Healthcare Information Exchange," *IEEE Journal of Biomedical and Health Informatics*, vol. 29, no. 9, pp. 6883–6891, Sep. 2025, , doi: 10.1109/JBHI.2025.3579722.

[33] D. Commey, S. G. Hounsinou, and G. V. Crosby, "Post-Quantum Secure Blockchain-Based Federated Learning Framework for Healthcare Analytics," *IEEE Networking Letters*, vol. 7, no. 2, pp. 126–129, Jun. 2025, , doi: 10.1109/LNET.2025.3563434.

[34] R. Razdan and M. J. Nene, "Post Quantum Signature for Blockchain," in *2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT)*. Belagavi, India: IEEE, Dec. 2025, pp. 1–5, , doi: 10.1109/ICAFT66710.2025.11453249.

[35] M. Chiranjeevi, N.Md. Bilal, J. A. I. S. Masood, N. S. Kalyan Chakravarthy, and N. Behera, "QUADRA - a Quantum-Resistant Distributed Resilient Architecture for Secure and Inclusive Digital Public Infrastructure," in *2025 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*. Kolhapur, India: IEEE, Oct. 2025, pp. 1–6, , doi: 10.1109/ICBDS67396.2025.11377033.

[36] A. Alsaeed, S. Almowuena, and A. N. Alyahya, "BAAIoV: A Blockchain-Based Authentication and Authorization Framework for Secure and Reliable Internet of Vehicles Communication," *IEEE Access*, vol. 13, pp. 150 821–150 837, 2025, , doi: 10.1109/ACCESS.2025.3601003.

[37] M. A. Aleisa, "Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT Environments," *IEEE Access*, vol. 13, pp. 18 660–18 676, 2025, , doi: 10.1109/ACCESS.2025.3529309.

[38] J. R, Z. A. K. N, and Devi. S, "Implementation of a Zero Trust Edge Blockchain Framework for IoT Security: Integrating 6G Connectivity and LoRaWAN," in *2025 International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication (IConSCEPT)*. Karaikal, India: IEEE, Dec. 2025, pp. 1–6, , doi: 10.1109/IConSCEPT66142.2025.11437031.

[39] E. Zeydan, L. Blanco, J. Mangues-Bafalluy, S. S. Arslan, and Y. Turk, "Post-Quantum Blockchain-Based Decentralized Identity Management for Resource Sharing in Open Radio Access Networks," *IEEE Transactions on Green Communications and Networking*, vol. 8, no. 3, pp. 895–909, Sep. 2024, , doi: 10.1109/TGCN.2024.3432689.

[40] H. Ghaemi and D. Abbasinezhad-Mood, "Novel Blockchain-Integrated Quantum-Resilient Self-Certified Authentication Protocol for Cross-Industry Communications," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 5, pp. 4493–4502, Sep. 2024, , doi: 10.1109/TNSE.2024.3428916.

[41] E. Zeydan, J. Baranda, and J. Mangues-Bafalluy, "Post-Quantum Blockchain-Based Secure Service Orchestration in Multi-Cloud Networks," *IEEE Access*, vol. 10, pp. 129 520–129 530, 2022, , doi: 10.1109/ACCESS.2022.3228823.

[42] Y. Gong and B.-J. Hu, "A Quantum-Resistant Key Management Scheme Using Blockchain in C-V2X," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 11, pp. 16 831–16 844, Nov. 2024, , doi: 10.1109/TITS.2024.3421381.

[43] X. Liu, H. Wang, W. Liu, L. Gong, and T. Liu, "APQE-CDA: A PUF-Based Post-Quantum End-to-End Cross-Domain Authenticated Key Agreement Protocol for IOD System," *IEEE Internet of Things Journal*, vol. 13, no. 4, pp. 7441–7462, Feb. 2026, , doi: 10.1109/JIOT.2025.3639219.

[44] G. Hao and J. Wu, "Efficient Post-Quantum Blockchain Transaction via Edge PUF-Enabled Persistent Verification in IoT," *IEEE Internet of Things Journal*, vol. 13, no. 2, pp. 1947–1962, Jan. 2026, , doi: 10.1109/JIOT.2025.3627770.

[45] H. M. S. Badar, S. Ahmed, N. I. Kajla, G. Fan, and C. Zhang, "Q-BLAISE: Quantum-Resilient Blockchain and AI-Enhanced Security Protocol for Smart Grid IoT," *IEEE Transactions on Consumer Electronics*, vol. 71, no. 2, pp. 4959–4971, May 2025, , doi: 10.1109/TCE.2025.3570969.

[46] Y. Liu, B. Zhao, X. Lin, Z. Guan, D. Li, J. Liu, Q. Wu, W. Susilo, and R. H. Deng, "Quantum-Resistant Sharding Blockchain and Its Application in Secure Data Transmission," *IEEE Journal on Selected Areas in Communications*, vol. 43, no. 8, pp. 2732–2746, Aug. 2025, , doi: 10.1109/JSAC.2025.3568043.

[47] C. Sun, N. M. Mahfuz, and Y. Wang, "Quantum-Resistant Privacy and Auditing for Blockchain: A Lattice-Based Approach With Composable Security," *IEEE Transactions on Dependable and Secure Computing*, vol. 23, no. 4, pp. 7610–7626, Jul. 2026, , doi: 10.1109/TDSC.2026.3674809.

[48] K. Sachdeva, "A Privacy-Focused, Post-Quantum-Oriented Digital Identity System Using Blockchain and Zero-Knowledge Proofs," *IEEE Access*, vol. 14, pp. 115 040–115 054, 2026, , doi: 10.1109/ACCESS.2026.3715111.

[49] C. Näther, D. Herzinger, S.-L. Gazdag, J.-P. Steghöfer, S. Daum, and D. Loebenberger, "Migrating Software Systems Toward Post-Quantum Cryptography-A Systematic Literature Review," *IEEE Access*, vol. 12, pp. 132 107–132 126, 2024, , doi: 10.1109/ACCESS.2024.3450306.

[50] F. Alsulami, "Adaptive-AI-Zerotrust-Chain: AI-Centric Zero Trust Enforcement for IoT Security," in *2026 IEEE 2nd International Conference on Secure IoT, Assured and Trusted Computing (SATC)*. Houston, TX, USA: IEEE, Mar. 2026, pp. 1–6, , doi: 10.1109/SATC69565.2026.11542301.

[51] K. Fayaz, V. Chakradhar, and U. D, "API Security with JWT Authentication and Reputation Based Monitoring System," in *2026 Fifth International Conference on Power, Control and Computing Technologies (ICPC2T)*. Raipur, India: IEEE, Mar. 2026, pp. 746–751, , doi: 10.1109/ICPC2T68221.2026.11646386.

[52] Y. Jang, H. Jang, and S. Lee, "A Quantum-Resistant and AI-Resilient Real-Time Keystroke Protection Framework With Blockchain-Backed Decentralized Identity," *IEEE Access*, vol. 14, pp. 57 879–57 894, 2026, , doi: 10.1109/ACCESS.2026.3680275.

[53] M. Sharma, R. Zaidi, and V. Sharma, "A Practical Quantum-Resistant Security Evaluation Framework for Blockchain Infrastructure," in *2026 International Conference on Connected Intelligence for Industrial Applications (CI2A)*. Punjab, India: IEEE, Apr.

2026, pp. 1–6, , doi: 10.1109/CI2A69097.2026.11577073.

[54] A. Shahidinejad and J. Abawajy, "Decentralized Lattice-Based Device-to-Device Authentication for the Edge-Enabled IoT," *IEEE Systems Journal*, pp. 1–11, 2023, , doi: 10.1109/JSYST.2023.3319280.

[55] S. Xu, T. Wang, A. Sun, Y. Tong, Z. Ren, R. Zhu, and H. H. Song, "Post-Quantum Anonymous, Traceable and Linkable Authentication Scheme Based on Blockchain for Intelligent Vehicular Transportation Systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 9, pp. 12 108–12 119, Sep. 2024, , doi: 10.1109/TITS.2024.3383668.

[56] D. Chaudhary, P. Santhi, M. S. P. Durgarao, A. Padmavathi, M. Mehedi Hassan, and B. Fahad Alkhamees, "Module Lattice-Based Post Quantum Secure Blockchain Empowered Authentication Framework for Autonomous Truck Platooning," *IEEE Access*, vol. 12, pp. 105 219–105 233, 2024, , doi: 10.1109/ACCESS.2024.3434691.

[57] R. R. Irshad, S. Hussain, I. Hussain, J. A. Nasir, A. Zeb, K. M. Alalayah, A. A. Alattab, A. Yousif, and I. M. Alwayle, "IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Blockchain-Based Approach Toward a Trustworthy Cloud Computing," *IEEE Access*, vol. 11, pp. 105 479–105 498, 2023, , doi: 10.1109/ACCESS.2023.3318755.

[58] S. P. Shanmugam, B. Subbiyan, K. Leelasankar, B. K. Mohanta, A. I. Awad, B. Mokhtar, and A. Y. Zomaya, "Lightweight Quantum-Resistant Blockchain-Based Key Agreement Scheme for IoV Communications," *IEEE Open Journal of the Communications Society*, vol. 7, pp. 3778–3799, 2026, , doi: 10.1109/OJCOMS.2026.3679308.

[59] A. Kumar, M. Malhotra, A. Anjali, and A. S. Yadav, "A Low-Latency Post-Quantum Group Authentication Framework for VANETs," *IEEE Networking Letters*, vol. 8, pp. 125–129, 2026, , doi: 10.1109/LNET.2026.3666683.

[60] F. Alanazi, M. Zareei, and M. García Martínez, "A Blockchain-Enabled Privacy-Preserving IoT Framework With Domain-Adaptive Anomaly Detection in Zero-Trust Environments," *IEEE Access*, vol. 13, pp. 206 883–206 895, 2025, , doi: 10.1109/ACCESS.2025.3624661.

[61] Z. Yang, H. Alfauri, B. Farkiani, R. Jain, R. Di Pietro, and A. Erbad, "A survey and comparison of post-quantum and quantum blockchains," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 2, pp. 967–1002, 2023, , doi: 10.1109/COMST.2023.3325761.

[62] X. Ren, M. Xu, D. Niyato, J. Kang, Z. Xiong, C. Qiu, H. Yao, and X. Wang, "Building resilient web 3.0 infrastructure with quantum information technologies and blockchain: an ambilateral view," *Proceedings of the IEEE*, vol. 112, no. 11, pp. 1686–1715, 2025, , doi: 10.1109/JPROC.2024.3520803.

[63] Y. Baseri, A. Hafid, Y. Shahsavari, D. Makrakis, and H. Khodaiemehr, "Blockchain security risk assessment in quantum era, migration strategies and proactive defense," *IEEE Communications Surveys & Tutorials*, 2025, , doi: 10.1109/COMST.2025.3621113.