Internet of Communicating Things (IoCT): A Decentralized, Post-Quantum Secure Architecture for Cooperative IoT Systems

Vishal Garg
NCOG Limited, 801 International Parkway Suite 500-118, Lake Mary, FL 32746, USA

***Abstract*—The Internet of Communicating Things (IoCT) extends the traditional Internet of Things (IoT) by making autonomous, peer-to-peer communication the primary paradigm: intelligent devices discover neighbors, propagate data and decisions through gossip-based dissemination, validate one another, and act locally in real time. This paper presents the IoCT reference architecture as three planes: a real-time communication-and-decision plane built on adaptive gossip protocols and embedded intelligence; a security plane specified as IoCT-KMS, a hierarchical post-quantum key-management scheme built on the NIST ML-KEM and ML-DSA standards and engineered for constrained links; and a pluggable trust-and-data plane that may reside entirely in enterprise infrastructure, anchor selected records to a distributed ledger, or use a natively relational, post-quantum ledger such as the NCOG Earth Chain Dual-Consensus Database. Shared state is managed with conflict-free replicated data types under strong eventual consistency, while a deterministic local safe-state override preserves functional-safety guarantees independent of network conditions. We analyze latency requirements from 3GPP, SAE, and industrial-safety standards to show why decisions of the safety and coordination classes must be made locally; quantify the on-air cost of post-quantum cryptography on IEEE 802.15.4 and LoRaWAN links; position the architecture against related systems and patents; and outline an evaluation plan. Supported by an extensive review of standards and peer-reviewed research, IoCT offers a scalable, self-healing, and quantum-resistant foundation for cooperative ecosystems of communicating things.**

***Index Terms*—Internet of Communicating Things (IoCT); decentralized IoT; gossip protocols; device-to-device communication; post-quantum cryptography; ML-KEM; ML-DSA; conflict-free replicated data types; blockchain; decentralized database.**

I. INTRODUCTION

The Internet of Communicating Things (IoCT) is an emerging paradigm that extends the traditional Internet of Things by enabling smart devices to communicate directly with each other and make cooperative decisions. In a conventional IoT deployment, devices stream data to centralized servers or cloud platforms, which analyze the data and issue control commands. This centralized model falters precisely where dependability matters most: if connectivity is lost or a hub fails, vital data never reaches the cloud and commands never return in time. IoCT addresses these weaknesses by fostering peer-to-peer communication among devices so that they can share data, monitor one another's status, and take local actions autonomously.

The defining invariant of IoCT is the *communication and propagation model*—not the data's final resting place. Persistent storage and trust anchoring are pluggable deployment choices: an IoCT system may persist data entirely within enterprise infrastructure, anchor selected records to a distributed ledger, or use a natively integrated decentralized database—without changing how devices communicate, decide, and cooperate.

II. CHALLENGES IN TRADITIONAL IOT SYSTEMS

Four structural weaknesses motivate the IoCT design. (1) *Reliance on continuous connectivity:* cloud-centric deployments assume sensors can always reach a remote server, yet connectivity is often intermittent or bandwidth-limited. (2) *Single points of failure:* a hub or cloud outage can idle an entire smart factory; a

solely responsible sensor can blind the system. (3) *Latency:* cloud round trips are incompatible with reactions that must occur within milliseconds. (4) *Data integrity and trust:* a malfunctioning or compromised device can inject incorrect data and induce bad decisions.

The Quantum Motivation

A fifth challenge is now unavoidable. The urgency of post-quantum migration rests on "harvest now, decrypt later": adversaries can capture ciphertext today and decrypt it once a cryptographically relevant quantum computer (CRQC) exists. Mosca's inequality formalizes the risk—if the required data-secrecy lifetime plus the migration time exceeds the time to a CRQC, exposure is unavoidable. NIST IR 8547 (initial public draft, November 2024) codifies the transition by deprecating quantum-vulnerable public-key algorithms (RSA, ECDSA, ECDH) after 2030 and disallowing them after 2035 [1]. The Global Risk Institute's 2024 Quantum Threat Timeline report, drawing on 32 experts, estimates a 19–34% probability of a CRQC within ten years [2]. IoT devices with 10–20-year field lifespans therefore fall squarely inside the risk window and must ship with post-quantum key establishment from day one, using the finalized NIST standards ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205) [3, 4, 5].

Contributions

This paper contributes: (1) a three-plane IoCT reference architecture with a pluggable trust plane spanning enterprise storage, ledger anchoring, and a natively relational post-quantum ledger; (2) IoCT-KMS, a hierarchical post-quantum key-management specification that confines kilobyte-scale signatures to join and rekey events so that steady-state gossip fits constrained frames; (3) a reference gossip communication profile with explicit storm-control parameters; (4) a consistency-and-safety model combining CRDT-managed shared state with a deterministic local safe-state override; (5) an integration design for the NCOG Dual-Consensus Database as a queryable, relational trust plane; and (6) an application analysis grounded in 3GPP, SAE, IEC, and U.S. Department of Energy sources.

III. BACKGROUND AND RELATED WORK

Gossip-Based Peer-to-Peer Communication

Gossip (epidemic) protocols disseminate information the way rumors spread: each node periodically shares state with a few randomly chosen neighbors until the information percolates through the network. The approach is decentralized, load-balanced, and fault-tolerant by construction, and its cost grows only logarithmically with network size: push–pull rumor spreading completes in $\log_3 n + O(\log \log n)$ rounds on a complete graph [6]. SWIM decouples failure detection from dissemination and achieves constant per-node message load independent of group size [7]; the Lifeguard extensions improve detection accuracy under stress [8], and production implementations default to a 200 ms gossip interval with a fanout of three [9]. Redundant transmissions are suppressed with the Trickle algorithm's polite-gossip mechanism (RFC 6206) [10]. For IoT specifically, Altoaimy et al. report that a context-aware, multi-factor weighted gossip protocol achieved substantially shorter end-to-end delay for critical IoT traffic and improved bandwidth utilization and network lifetime versus traditional gossiping and FELGossiping; the gains are presented graphically rather than as summary percentages [11]. Epidemic broadcast trees such as Plumtree further reduce message overhead for large payloads [12].

Post-Quantum Cryptography on Constrained Devices

NIST finalized ML-KEM, ML-DSA, and SLH-DSA in August 2024 [3, 4, 5]; FN-DSA (Falcon) remains a draft (FIPS 206), with final publication expected in late 2026 or early 2027 [13]. Table I lists the finalized parameter sizes. Feasibility on microcontrollers is established: the pqm4 benchmarking framework provides Cortex-M4 cycle counts for all schemes [14], and a recent study on the ARM Cortex-M0+ (RP2040, 133 MHz) measured a full ML-KEM-512 key exchange in 35.7 ms consuming 2.83 mJ—17× faster than ECDH P-256 on the same hardware—while also documenting high ML-DSA signing variance due to rejection sampling [15]. The binding constraint is the air interface rather than computation: IEEE 802.15.4 frames carry roughly 102 usable bytes [16], and LoRaWAN application payloads range from 51 bytes at DR0 to 222–242 bytes at higher data rates [17]. Hybrid classical-plus-post-quantum key exchange is

standardizing rapidly: X25519MLKEM768 for TLS 1.3 has received IESG approval and awaits publication in the RFC Editor queue [18], while EDHOC (RFC 9528) provides the lightweight authenticated-key-exchange baseline for constrained devices [19]. For group communication, MLS (RFC 9420) defines scalable group keying [20], with post-quantum ciphersuites progressing as IETF working-group drafts [21].

TABLE I FINALIZED NIST PQC PARAMETER SIZES (BYTES)

Scheme	Public key	Private key	Sig. / Ciphertext
ML-DSA-44	1,312	2,560	2,420 (sig)
ML-DSA-65	1,952	4,032	3,309 (sig)
ML-DSA-87	2,592	4,896	4,627 (sig)
ML-KEM-512	800	1,632	768 (ct)
ML-KEM-768	1,184	2,400	1,088 (ct)
ML-KEM-1024	1,568	3,168	1,568 (ct)
SLH-DSA-128s	32	64	7,856 (sig)

Distributed Ledgers and Decentralized Databases for IoT

Distributed-ledger designs relevant to IoT include leaderless asynchronous BFT consensus over directed acyclic graphs (DAGs), exemplified by hashgraph [22], and the evolving IOTA platform, which after its 2025 "Rebased" upgrade adopted delegated proof of stake with sub-second finality but abandoned feeless transactions [23]. On the post-quantum front, the Quantum Resistant Ledger has used hash-based XMSS signatures since 2018 [24], and Algorand deployed Falcon-based State Proofs in 2022 and reports its first Falcon-1024-secured mainnet transaction on November 3, 2025, with native post-quantum accounts on the Foundation roadmap for Q3 2026 [25]. In parallel, decentralized *databases* have emerged: Kwil provides community-operated PostgreSQL-based SQL networks [26]; Space and Time couples an off-chain data warehouse with a zero-knowledge Proof-of-SQL prover [27]; and peer-reviewed systems such as SEBDB [28] and FalconDB [29] add relational semantics and SQL querying to blockchain storage. NCOG Earth Chain integrates a relational data layer directly at Layer-1: its Dual-Consensus Database (DDB), based on PostgreSQL, endorses SQL transactions through a local BFT phase and finalizes them through the chain's global consensus [30]. Section VII details how IoCT uses this class of trust plane.

Related Patents and Positioning

The closest patent family covers distributed IoT device communication and distributed acting and knowledge: US 11,757,894 B2 ("Distributed communication between Internet of Things devices") and US 10,375,079 B2 ("Distributed acting and knowledge for the Internet of Things"), both assigned to McAfee, LLC [31, 32]. US 10,855,655 B2 (Unisys) secures IoT collections through communities of interest sharing common encryption keys [33], and US 12,107,966 B2 (Ceremorphic) describes blockchain-based lightweight device authentication [34]. None of these—nor, to our knowledge, any published system—unifies adaptive gossip dissemination, embedded-AI local autonomy, NIST post-quantum key management engineered for constrained links, and an asynchronous relational trust plane. IoCT's contribution is precisely this integrated architecture.

IoCT Reference Architecture

IoCT is organized as three planes (Fig. 1).

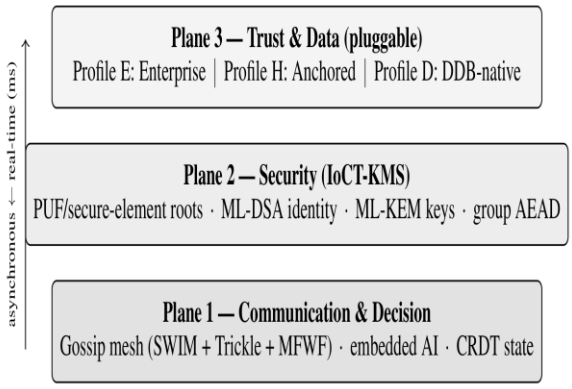

Fig. 1. The IoCT three-plane reference architecture. Latency-critical decisions never leave Plane 1; the trust plane is a deployment choice.

TABLE II TRUST-PLANE DEPLOYMENT PROFILES

Profile	Trust root / persistence	When to use
E	Enterprise PKI; enterprise DB, historian, or data lake	Single-organization deployments; data sovereignty; existing IT estate
H	Enterprise PKI + ledger-anchored digests, revocations, firmware hashes	Auditability and tamper evidence without on-chain data
D	Ledger-registered identities; structured records in the NCOG DDB; bulk telemetry off-chain	Multi-party ecosystems needing shared, queryable, tamper-evident records with post-quantum protection

Plane 1 — Communication and Decision (mandatory). A context-aware gossip mesh (Section IV) combined with embedded AI or rule engines. All latency-critical actions—safety responses, predictive-maintenance triggers, cooperative coordination—resolve here, in the mesh, in milliseconds.

Plane 2 — Security (mandatory). Post-quantum device identity, authenticated group admission, encrypted group communication, and revocation, specified as IoCT-KMS (Section V).

Plane 3 — Trust and Data (pluggable). Three deployment profiles (Table II) let the same mesh operate against different persistence and trust backends. Profile E keeps all data in enterprise infrastructure; Profile H adds tamper evidence by anchoring digests, revocations, and firmware hashes to a ledger; Profile D registers identities and audit-grade records in a natively relational ledger database.

Data is partitioned into four classes with fixed placement rules: Class A operational state (live status, alarms, coordination) lives only in the mesh, CRDT-managed and ephemeral; Class B high-rate telemetry is buffered at the edge and persisted to an enterprise historian in all profiles—never on-chain; Class C audit-grade records (identity, commissioning, key events, maintenance provenance, decision logs) go to the enterprise database (E), additionally anchored (H), or to DDB tables (D); and Class D cross-organizational proofs and settlement exist only in Profiles H and D.

Communication Layer: The IoCT Gossip Profile

The reference profile IoCT-GCP v1.0 fixes concrete, tunable defaults. Membership and failure detection use SWIM with Lifeguard: a 200 ms protocol period on IP meshes (1 s on constrained wireless), fanout of three, and a suspicion timeout of three to five periods [7, 8, 9]. Dissemination uses push–pull rumor mongering with age-counter retirement, giving expected propagation in $O(\log n)$ rounds [6]. Message scheduling applies context-aware multi-factor weighting in the spirit of [11]—message priority, residual energy, and node distance and density—with the safety class preempting all queues. Storm control uses Trickle with redundancy constant $k = 2$, $I_{min} = 125$ ms, and $I_{max} = I_{min} \times 2^{10}$, plus a duplicate-suppression cache [10]. The profile binds to UDP/IPv6 over Thread, Wi-Fi, or Ethernet; to 6LoWPAN over IEEE 802.15.4; and to BLE, with payloads sized to a single frame wherever possible—a property the key-management design makes achievable. Gossip delivery is probabilistic rather than deterministic; the safety consequences of this are addressed in Section VI. Convergence at target fleet sizes is to be validated in simulation (Section IX).

IV. SECURITY ARCHITECTURE: IOCT-KMS V1.0

Roots of Trust and Provisioning

Every device receives, at manufacture or commissioning, a hardware-rooted *Device Identity Key* (DIK)—an ML-DSA keypair whose private key is generated and stored in a secure element, TrustZone/eFUSE, or regenerated on demand from a physical unclonable function (PUF) and never stored at rest where a PUF is available. A signed registration record (device ID, public key, tier, manufacturer, commissioning time) is written to the trust plane of the active profile.

Two-Tier Algorithm Suite

Table III defines two tiers. Tier-G (gateways, edge servers, controllers) uses ML-KEM-1024, ML-DSA-87, AES-256-GCM, and SHA-3-384—aligned with the NSA CNSA 2.0 suite [35] and with the algorithm choices NCOG documents for its chain [30], yielding one coherent cryptographic story across mesh and ledger. Tier-C (constrained MCUs and sensors) uses ML-KEM-768, ML-DSA-65, and AES-256-GCM or

ASCON, the NIST lightweight-cryptography selection currently specified in draft SP 800-232 [36]. Where classical interoperability is required during transition, hybrid X25519+ML-KEM establishment is used [18].

TABLE III IOCT-KMS ALGORITHM SUITE

	Tier-G (gateway)	Tier-C (constrained)
KEM	ML-KEM-1024	ML-KEM-768
Signature	ML-DSA-87 (4,627 B)	ML-DSA-65 (3,309 B)
AEAD	AES-256-GCM	AES-256-GCM / ASCON
Hash	SHA-3-384	SHA-3-256
Transition	Hybrid X25519 + ML-KEM	

Key Hierarchy and Join Protocol

The hierarchy is: DIK (device lifetime, hardware-rooted) → pairwise session key PSK (ML-KEM-established; rotated at most every 7 days or on demand) → group traffic key GTK (256-bit symmetric; rotated at most every 24 h *and* immediately on any membership change) → per-message AEAD nonce and sequence number with a replay window.

Admission proceeds in five steps. (1) The joining device sends an ML-DSA-signed Join Request containing its identity certificate or registration reference, capabilities, and a nonce. (2) The group controller—or any authorized member—verifies the signature *and* checks registration and revocation state in the trust plane; this closed admission is the Sybil defense. (3) The controller performs ML-KEM encapsulation to the device's public key, establishing the PSK, and returns a signed Join Accept. (4) The current GTK is delivered under the PSK. (5) Thereafter, all gossip traffic is protected by AEAD under the GTK with sequence numbers—no kilobyte-scale signatures on the air per message.

On-Air Cost Analysis

Signatures are confined to join and rekey events. The one-time join cost—an ML-DSA-65 signature (≈3.3 kB) plus an ML-KEM-768 ciphertext (≈1.1 kB)—amounts to roughly 45 fragments on IEEE 802.15.4 (≈102 usable bytes per frame) [16] and is acceptable once per join or rekey. Steady-state gossip messages carry only an AEAD tag and sequence number—tens of bytes of overhead—and fit in single frames. On LoRaWAN, whose payloads range from 51 bytes at DR0 to 222–242 bytes at higher rates [17], the same analysis motivates confining post-quantum objects to key establishment and keeping signatures off the air interface in steady state.

Rekeying, Revocation, and Fallback

Rekey triggers are timer expiry, any membership change, and suspected compromise. Upon revocation, a signed revocation record propagates through the mesh via gossip and is written to the trust plane, and an immediate group rekey excludes the revoked device. Forward secrecy derives from fresh ML-KEM encapsulations at every rotation; a compromised GTK exposes at most one rotation window (≤24 h). Pre-embedded symmetric keys are permitted only for Tier-C devices with short deployment lifetimes; they must be unique per device (never fleet-wide), carry a mandatory expiry, and migrate to the full hierarchy when hardware allows.

Threat Model

Table IV summarizes the adversary model and mitigations, including the harvest-now-decrypt-later quantum adversary that motivates the suite in Table III.

Consistency and Safety

Shared mesh state uses conflict-free replicated data types (CRDTs), which guarantee strong eventual consistency without coordination [37]: OR-Sets for group membership and neighbor sets, LWW-Registers for device status and configuration, PN-Counters for aggregates, and G-Sets for append-only alarm and event logs. Causality is tracked with version vectors [38, 39, 40]. CRDT feasibility on constrained edge hardware has been demonstrated by the Achlys framework running the Lasp CRDT library on embedded boards [41].

Because gossip delivery is probabilistic, safety cannot depend on it. The architecture therefore adopts the following rule verbatim:

Mesh-shared state is advisory for the safety class and authoritative only for the coordination class. Every actuator enforces a deterministic local safe-state override that fires within the applicable process safety time (IEC 61508) regardless of mesh convergence, ledger availability, or network partition. Information

received via gossip may cause a device to enter its safe state earlier; it can never delay, veto, or loosen a locally determined safe action.
This decouples best-effort situational awareness from hard functional-safety guarantees and defines the certification pathway under IEC 61508 [42].

V. TRUST AND DATA PLANE

Enterprise-First Pluggability

Many deployments neither need nor want a ledger; Profile E is therefore a first-class citizen, with the trust plane realized by enterprise PKI and databases. Profile H adds tamper evidence at minimal cost by periodically anchoring Merkle digests of Class-C records, revocation lists, and firmware hashes. Profile D is designed for multi-party ecosystems in which no single organization is trusted to hold the authoritative record.

Integration with the NCOG Dual-Consensus Database

NCOG Earth Chain departs from sequential block-producing designs: its native Forest Protocol is a leaderless, asynchronous Byzantine Fault Tolerant (aBFT) consensus over a DAG of events, allowing validators to process and confirm transactions in parallel rather than through a single serialized block pipeline [30]. The Dual-Consensus Database extends this with a two-phase data path—local BFT endorsement of SQL transactions followed by global DAG-aBFT finalization—a structure designed to remove the throughput bottleneck of conventional chains and deliver near-real-time confirmation for on-chain data operations. Specific throughput and finality figures are as reported by NCOG pending publication of the benchmark methodology. Importantly, IoCT's real-time guarantees do not depend on ledger latency: all safety- and latency-critical decisions are made locally in the mesh (Section VI), so the trust plane's speed determines how quickly records become queryable and final—a property the
DDB's parallel architecture is specifically designed to maximize—never whether a machine acts in time.
Because the DDB is relational (PostgreSQL-based) [30], the trust plane holds queryable structured records rather than opaque hashes. The reference schema is:

TABLE IV IOCT THREAT MODEL AND MITIGATIONS

Adversary	Capability	Mitigation
Passive eavesdropper, incl. harvest-now-decrypt-later quantum adversary	Records all traffic for future decryption	ML-KEM key establishment + AEAD; post-quantum suite sized for 10–20-year device lifetimes [1]
Message injector / spoofing	Sends forged gossip	AEAD under the GTK; ML-DSA-authenticated join; unauthenticated frames dropped
Sybil attacker	Floods mesh with fake identities	Closed admission: join requires a registered, non-revoked identity in the trust plane; no open joins
Compromised legitimate device	Holds valid keys; behaves maliciously	Revocation + immediate group rekey; reputation and anomaly flags in the trust plane; blast radius ≤ one GTK window
Replay attacker	Re-sends captured valid messages	Per-message sequence numbers with replay window
DoS / gossip-storm attacker	Amplifies traffic	Trickle suppression, fanout caps, rate limits, duplicate cache [10]
Malicious insider at enterprise/cloud	Tampers with stored records	Profiles H/D: anchored digests or ledger immutability make tampering evident; mesh traffic is end-to-end protected independent of backend

```
device_registry(device_id PK, mldsa_pubkey,
  tier, manufacturer, model, commissioned_at,
  status, group_id)
key_events(event_id PK, device_id FK,
  event_type, gtk_epoch, occurred_at, signed_by)
maintenance_log(entry_id PK, device_id FK,
  detected_by, anomaly_class, action_taken,
  mesh_decision_latency_ms, occurred_at)
reputation(device_id FK, score, last_updated,
  computed_from)
firmware(device_model, version, image_hash,
  signed_manifest, released_at)
```

Queries impossible with hash-anchoring alone become native: the full maintenance provenance of a machine across owners; all devices still running firmware below a given version, ordered by commissioning date; or the revocation history of a group. In Profiles E and H the same schema lives in the enterprise database, with Profile H adding periodic digest anchoring.

Decentralized SQL databases exist as standalone networks [26] and as layers over existing chains [27], and relational-on-blockchain systems have been demonstrated academically [28, 29]. NCOG's design is differentiated by combining native Layer-1 relational integration, DAG-based asynchronous BFT consensus, and post-quantum cryptography (ML-DSA-87, ML-KEM-1024) within a single stack—a combination we have not found in any other production system.

VI. APPLICATIONS AND BENEFITS

Why Decisions Must Be Local

Table V compiles latency requirements from primary standards. 5G ultra-reliable low-latency communication targets 1 ms user-plane latency at 99.999% reliability [43]; URLLC use cases in factory automation, smart grid, and transportation span 1–10 ms with residual error rates of 10^{-4} to 10^{-9} [44]; enhanced-V2X requirements reach 3 ms end-to-end for the most demanding advanced-driving scenarios [45]; and SAE J2945/1 sets a nominal 10 Hz (100 ms) basic-safety-message cadence [46]. No cloud round trip—and no global ledger—can sit inside these loops; the gossip mesh with local intelligence can.

TABLE V LATENCY REQUIREMENTS BY APPLICATION CLASS

Application class	Target	Source
5G URLLC (user plane)	1 ms, 99.999%	3GPP TS 22.261 [43]
Process-automation remote control	50 ms e2e, 99.9999%	3GPP TS 22.261 [43]
Factory / grid / ITS (URLLC span)	1–10 ms	3GPP TR 22.862 [44]
Advanced driving / platooning	3–10 ms	3GPP TS 22.186 [45]
V2X basic safety message	100 ms (10 Hz)	SAE J2945/1 [46]
PQC key exchange, Cortex-M0+	35.7 ms (measured)	[15]

Predictive and Preventive Maintenance

Neighboring machines collaboratively validate anomalies—vibration, thermal, or acoustic signatures—and trigger interventions within the mesh. The economic case is grounded in the U.S. Department of Energy's Operations and Maintenance Best Practices Guide: a properly functioning predictive-maintenance program yields 8–12% savings over preventive maintenance alone, with opportunities exceeding 30–40% relative to reactive maintenance [47]. Every intervention is recorded as Class-C provenance, giving auditable maintenance histories that survive changes of ownership.

Further Domains

Critical safety: emergency shutdown and interlock coordination execute locally under the Section VI rule, with the trust plane providing the audit trail. *Smart manufacturing:* interdependent cells synchronize through the mesh; a fault detected by one robot propagates to its neighbors in $O(\log n)$ gossip rounds. *Energy and smart grid:* local dispatch decisions pair with Profile-D settlement for peer-to-peer energy accounting. *Vehicles:* V2X cooperation at the cadences of Table V, with ledger-based identity and revocation. *Healthcare and wearables:* on-body device groups corroborate distress signals before alerting caregivers. *Military and disaster relief:* brokerless gossip keeps units connected when infrastructure is destroyed, so that missions do not stop when networks fail [48], while the post-quantum suite protects long-lived secrets.

VII. EVALUATION PLAN, CHALLENGES, AND COMPLIANCE

Evaluation Plan

Three measurements will substantiate the reference profiles: (1) pqm4- and liboqs-based ML-KEM/ML-DSA latency and energy runs on the target Cortex-M4/M33-class hardware [14]; (2) gossip convergence and storm-control behavior at target fleet sizes in Contiki-NG/Cooja or ns-3, under IEEE 802.15.4 fragmentation; and (3) measured anchoring latency of Class-C records against a live testnet for Profiles H and D.

Challenges

Interoperability: IoCT is an overlay. It complements Matter—which covers commissioning and controller-based local control, with Thread as a shared transport [49]—by adding autonomous device-to-device coordination beyond the controller model; device capabilities can be described with W3C Web of Things Thing Descriptions 1.1 [50]. *Consistency:* strong eventual consistency provides convergence but no timeliness bound; the safety override of Section VI is therefore not optional. *Standards in flight:* FN-DSA remains draft FIPS 206 [13]; the TLS hybrid and SUIT manifest specifications are in the RFC Editor queue [18, 51]; MLS post-quantum ciphersuites are working-group drafts [21]; NIST IR 8547 is an initial public draft [1]; deployments should pin exact draft versions. *Vendor verification:* the DDB's performance characteristics are vendor-reported pending publication of an architecture specification and benchmark methodology; Profile-D adopters should require both.

Regulatory Alignment

The design maps onto the emerging compliance landscape: ETSI EN 303 645 (V3.1.3, 2024) and NIST IR 8425 baselines for device security [52, 53]; IETF SUIT for signed firmware updates [51]; the EU Cyber Resilience Act (Regulation (EU) 2024/2847), in force since December 10, 2024, with reporting obligations from September 11, 2026 and full application from December 11, 2027 [54]; and the NIST IR 8547 post-quantum timeline (deprecation after 2030, disallowance after 2035) [1] together with CNSA 2.0 milestones for high-assurance systems [35].

VIII. CONCLUSION

The Internet of Communicating Things reframes the IoT around what devices *do together*: discover one another, gossip state, validate claims, decide locally, and record what matters. This paper specified that vision as an implementable architecture—a tuned gossip profile, a post-quantum key-management scheme that respects constrained frames, a CRDT-based consistency model with a deterministic safety override, and a trust plane that scales from an enterprise database to a natively relational, post-quantum ledger. IoCT's contribution is the integrated architecture: CRDT-managed shared state over an adaptive gossip mesh, post-quantum device identity and group keying designed for constrained links, embedded-AI local autonomy with a deterministic safe-state override, and a pluggable trust plane ranging from enterprise storage to a natively relational, post-quantum ledger—a combination we have not found unified in any prior system or patent. Its limitations are stated openly: gossip is probabilistic, several supporting standards are still drafts, and ledger performance claims await independent benchmarks. Within those bounds, IoCT offers a credible, standards-aligned path from isolated devices to a cooperative, quantum-resistant ecosystem of communicating things.

REFERENCES

[1] NIST, "Transition to post-quantum cryptography standards," NIST IR 8547 (Initial Public Draft), Nov. 2024.
[2] M. Mosca and M. Piani, "Quantum threat timeline report 2024," Global Risk Institute / evolutionQ, Dec. 2024.
[3] NIST, "Module-lattice-based key-encapsulation mechanism standard," FIPS 203, Aug. 2024.
[4] NIST, "Module-lattice-based digital signature standard," FIPS 204, Aug. 2024.
[5] NIST, "Stateless hash-based digital signature standard," FIPS 205, Aug. 2024.
[6] R. Karp, C. Schindelhauer, S. Shenker, and B. Vöcking, "Randomized rumor spreading," in *Proc. IEEE FOCS*, 2000, pp. 565–574.
[7] A. Das, I. Gupta, and A. Motivala, "SWIM: Scalable weakly-consistent infection-style

process group membership protocol," in *Proc. IEEE DSN*, 2002, pp. 303–312.

[8] A. Dadgar, J. Phillips, and J. Currey, "Lifeguard: Local health awareness for more accurate failure detection," in *Proc. IEEE/IFIP DSN-W*, 2018.

[9] HashiCorp, "memberlist: Golang package for gossip-based cluster membership," https://github.com/hashicorp/memberlist (accessed Aug. 2026).

[10] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko, "The Trickle algorithm," IETF RFC 6206, Mar. 2011.

[11] L. Altoaimy, A. Alromih, S. Al-Megren, G. Al-Hudhud, H. Kurdi, and K. Youcef-Toumi, "Context-aware gossip-based protocol for Internet of Things applications," *Sensors*, vol. 18, no. 7, art. 2233, 2018.

[12] J. Leitão, J. Pereira, and L. Rodrigues, "Epidemic broadcast trees," in *Proc. IEEE SRDS*, 2007, pp. 301–310.

[13] NIST, "FN-DSA (draft FIPS 206)," Initial Public Draft, Aug. 2025; final publication expected late 2026 / early 2027.

[14] M. J. Kannwischer et al., "pqm4: Testing and benchmarking NIST PQC on ARM Cortex-M4," https://github.com/mupq/pqm4 (benchmarks table accessed Aug. 2026).

[15] S. Chhetri et al., "Benchmarking NIST-standardised ML-KEM and ML-DSA on ARM Cortex-M0+," arXiv:2603.19340, 2026.

[16] IEEE, "IEEE standard for low-rate wireless networks," IEEE Std 802.15.4-2020.

[17] LoRa Alliance, "RP002-1.0.2 LoRaWAN regional parameters," 2020.

[18] IETF TLS WG, "X25519MLKEM768 hybrid key exchange for TLS 1.3," draft-ietf-tls-ecdhe-mlkem (IESG-approved; RFC Editor queue), 2026.

[19] G. Selander, J. Preuss Mattsson, and F. Palombini, "Ephemeral Diffie–Hellman over COSE (EDHOC)," IETF RFC 9528, Mar. 2024.

[20] R. Barnes et al., "The Messaging Layer Security (MLS) protocol," IETF RFC 9420, Jul. 2023.

[21] IETF MLS WG, "ML-KEM and hybrid cipher suites for MLS," draft-ietf-mls-pq-ciphersuites (work in progress), 2026.

[22] L. Baird, "The Swirlds hashgraph consensus algorithm: Fair, fast, Byzantine fault tolerance," Swirlds Tech. Rep. TR-2016-01, 2016.

[23] A. Carelli et al., "The evolution of the IOTA protocol," *Sensors*, vol. 25, no. 11, art. 3408, 2025.

[24] P. Waterland, "The Quantum Resistant Ledger," QRL whitepaper, 2018.

[25] Algorand Foundation, "Quantum-resistant transactions on Algorand with Falcon signatures," technical brief, 2025–2026 (native post-quantum accounts: Foundation roadmap, Q3 2026).

[26] Kwil, "The decentralized SQL database," https://www.kwil.com (accessed Aug. 2026).

[27] Space and Time, "Proof of SQL," technical documentation, 2025.

[28] Y. Zhu, Z. Zhang, C. Jin, A. Zhou, and Y. Yan, "SEBDB: Semantics empowered blockchain database," in *Proc. IEEE ICDE*, 2019, pp. 1820–1831.

[29] Y. Peng, M. Du, F. Li, R. Cheng, and D. Song, "FalconDB: Blockchain-based collaborative database," in *Proc. ACM SIGMOD*, 2020, pp. 637–652.

[30] NCOG, "NCOG Earth Chain documentation: Forest Protocol and the Dual-Consensus Database," https://docs.ncog.earth (accessed Aug. 2026).

[31] G. G. Infante-Lopez and R. J. Firby, "Distributed communication between Internet of Things devices," U.S. Patent 11,757,894 B2, McAfee, LLC, 2023.

[32] G. G. Infante-Lopez and R. J. Firby, "Distributed acting and knowledge for the Internet of Things," U.S. Patent 10,375,079 B2, McAfee, LLC, 2019.

[33] M. Entezari, C. Dremann, and J. Landis, "System and method for providing secure and redundant communications and processing for a collection of Internet of Things (IoT) devices," U.S. Patent 10,855,655 B2, Unisys Corp., 2020.

[34] A. Shrivastava et al., "Device authentication using blockchain," U.S. Patent 12,107,966 B2, Ceremorphic, Inc., 2024.

[35] NSA, "Commercial National Security Algorithm Suite 2.0," Cybersecurity Advisory, Sep. 2022 (updated May 2025).

[36] NIST, "Ascon-based lightweight cryptography standards," draft SP 800-232, 2024.

[37] M. Shapiro, N. Preguiça, C. Baquero, and M. Zawirski, "Conflict-free replicated data types," in *Proc. SSS*, LNCS 6976, 2011, pp. 386–400; also INRIA RR-7687.

[38] L. Lamport, “Time, clocks, and the ordering of events in a distributed system,” *Commun. ACM*, vol. 21, no. 7, pp. 558–565, 1978.

[39] C. J. Fidge, “Timestamps in message-passing systems that preserve the partial ordering,” in *Proc. 11th Australian Computer Science Conf.*, 1988, pp. 56–66.

[40] F. Mattern, “Virtual time and global states of distributed systems,” in *Parallel and Distributed Algorithms*, North-Holland, 1989, pp. 215–226.

[41] I. Kopestenski and P. Van Roy, “Achlys: Towards a framework for distributed storage and generic computing applications for wireless IoT edge networks with Lasp on GRiSP,” in *Proc. IEEE PerCom Workshops*, 2019, pp. 875–881.

[42] IEC, “Functional safety of electrical/electronic/programmable electronic safety-related systems,” IEC 61508, ed. 2.0, 2010.

[43] 3GPP, “Service requirements for the 5G system,” TS 22.261.

[44] 3GPP, “Feasibility study on new services and markets technology enablers for critical communications,” TR 22.862.

[45] 3GPP, “Enhancement of 3GPP support for V2X scenarios,” TS 22.186 (V18.0.1, 2024).

[46] SAE International, “On-board system requirements for V2V safety communications,” SAE J2945/1, rev. Apr. 2020.

[47] U.S. Dept. of Energy / Pacific Northwest National Laboratory, “Operations and maintenance best practices: A guide to achieving operational efficiency,” Release 3.0.

[48] Raft LLC, “How gossip keeps the warfighter connected when the network’s down,” https://teamraft.com (accessed Aug. 2026).

[49] Connectivity Standards Alliance, “Matter specification,” version 1.4, Nov. 2024.

[50] W3C, “Web of Things (WoT) Thing Description 1.1,” W3C Recommendation, Dec. 5, 2023.

[51] B. Moran, H. Tschofenig, D. Brown, and M. Meriac, “A firmware update architecture for Internet of Things,” IETF RFC 9019, Apr. 2021 (manifest specification in the RFC Editor queue, 2026).

[52] ETSI, “Cyber security for consumer Internet of Things: Baseline requirements,” EN 303 645 V3.1.3, Sep. 2024.

[53] NIST, “Profile of the IoT core baseline for consumer IoT products,” NIST IR 8425, Sep. 2022.

[54] European Union, “Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act),” in force Dec. 10, 2024.