Preprints.org

Article

Not peer-reviewed version

TRUST-Court: Tamper-Resistant Records for Universal Secure Transparency in Digital Judiciary Systems

Basker Palaniswamy *

Posted Date: 6 March 2026

doi: 10.20944/preprints202603.0442.v1

Keywords:
blockchain; digital signatures; post-quantum cryptography; ML-DSA; ML-KEM; SLH-DSA; storage optimization; e-judiciary

Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Article

TRUST-Court: Tamper-Resistant Records for Universal Secure Transparency in Digital Judiciary Systems

Basker Palaniswamy

Insight Research Ireland Centre for Data Analytics, Department of Computer Science and I.T., University College Cork (UCC), Cork City, Ireland, European Union; basker170889@zohomail.eu

Abstract

What if a court verdict could never be altered—not today, not tomorrow, and not even in the age of quantum computers? This paper introduces **TRUST-Court**, a next-generation digital judiciary framework that makes court records **tamper-proof, transparent, and quantum-secure**. Every participant in a case—plaintiff, defendant, lawyer, and judge—receives a verified digital identity and signs court proceedings using **post-quantum cryptographic algorithms standardized by NIST in 2024**. Hearings are transcribed in real time, digitally signed by all parties, and permanently sealed using multi-layer cryptographic protection before being anchored to a blockchain for public verification. The system integrates permissioned blockchain infrastructure (Hyperledger Fabric), public verification anchoring (Polygon), and post-quantum cryptographic primitives including **ML-DSA, ML-KEM, SLH-DSA, SHA-3, and AES-256**. To address the large data sizes of post-quantum signatures, we introduce practical storage optimization techniques such as Merkle-tree batching, signature aggregation, and archival compression, achieving **60–80% storage reduction** while preserving security guarantees. Through case studies from the United States, India, and Ireland, TRUST-Court demonstrates how judicial records can become mathematically verifiable public artifacts. By preventing document tampering, eliminating transcript disputes, and enabling citizen-level verification of verdicts, the framework offers a pathway toward a judiciary where **truth, once recorded, becomes permanently unalterable**.

Keywords: blockchain; digital signatures; post-quantum cryptography; ML-DSA; ML-KEM; SLH-DSA; storage optimization; e-judiciary

1. Introduction

The judiciary is the cornerstone of democratic governance, yet it remains one of the least digitized institutions globally. In the United States, federal and state courts process over 80 million cases annually, with an average civil case lifecycle exceeding 25 months. India faces an even more acute crisis, with over 50 million pending cases across its three-tier court hierarchy. Document tampering, transcript disputes, and delayed publication of verdicts erode public trust and undermine the rule of law.

To understand the problem in everyday terms, consider what happens today when a court verdict is delivered. A judge writes or dictates a judgment. That document is typed, printed, filed in a registry, and sometimes uploaded to a government website. At any point in this chain, the document can be altered—intentionally or accidentally—and there is no simple, mathematical way for a citizen to verify whether the published verdict is exactly what the judge signed. In high-profile cases, allegations of "missing pages" or "altered paragraphs" are not uncommon, and they can take months or years to resolve. For ordinary citizens, this means that the very institution meant to deliver justice cannot always prove that its own records are authentic.

Recent advances in cryptographic engineering and distributed ledger technology present a transformative opportunity. Digital signatures provide mathematical guarantees of authenticity and non-repudiation—meaning that if a judge signs a document digitally, it becomes mathematically

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

impossible to alter even a single character without detection. Blockchain networks offer immutable, auditable records without reliance on any single trusted authority. Together, these technologies can give every citizen the ability to independently verify that a court record is genuine, complete, and unchanged.

Critically, the emergence of **cryptographically relevant quantum computers (CRQCs)** poses an existential threat to classical public-key cryptography: RSA, ECDSA, and EdDSA will all be broken by Shor's algorithm. The implication for judicial systems is severe—an adversary could, in the future, forge digital signatures on court records that were signed with today's classical algorithms. Intelligence agencies are already believed to be stockpiling encrypted communications and signed documents in anticipation of quantum decryption capabilities, a strategy known as "harvest now, decrypt later." Judicial records—which must remain verifiable for decades—demand **post-quantum security from day one**.

In August 2024, NIST finalized three post-quantum standards: **ML-DSA** (FIPS 204, lattice-based signatures), **ML-KEM** (FIPS 203, lattice-based key encapsulation), and **SLH-DSA** (FIPS 205, hash-based signatures). These represent the culmination of an eight-year international effort and form the cryptographic foundation of TRUST-Court.

However, post-quantum cryptographic algorithms introduce a practical challenge: **significantly larger key and signature sizes**. For example, a single ML-DSA-65 signature is 3,293 bytes (compared to 64 bytes for Ed25519), and an SLH-DSA-192f signature is 35,664 bytes. When a judiciary system processes millions of cases per year, each with multiple signed transcripts and verdicts, the cumulative storage burden becomes substantial. This paper addresses this challenge head-on, proposing storage optimization strategies that reduce the footprint by 60–80% without compromising security.

Our contributions include:

1. A **post-quantum enrollment protocol** linking verified identities to ML-DSA/SLH-DSA signing keys and ML-KEM encapsulation keys.
2. A **multi-party hybrid PQ signature scheme** for court transcript signing with formal security analysis.
3. A **hybrid blockchain architecture** combining Hyperledger Fabric with Polygon PoS for national-scale deployment.
4. **Storage optimization techniques** for post-quantum cryptographic data, achieving 60–80% reduction in storage requirements.
5. **Case studies** for the USA, India, and Ireland, including a detailed Irish traffic offence courtroom walkthrough.
6. A **formal cryptographic research roadmap** identifying eleven open problems and attractive directions for the cryptographic community.
7. A **phased national transition roadmap** with formal post-quantum security proofs.

2. The Quantum Threat to Judicial Records

This section explains why quantum computers threaten the security of court records and why action must be taken now, even though large-scale quantum computers may still be years away.

2.1. What Is a Quantum Computer?

A classical computer stores information as bits—each bit is either 0 or 1. A quantum computer uses *qubits*, which can exist in a combination (superposition) of 0 and 1 simultaneously. This allows quantum computers to explore many possible solutions in parallel for certain mathematical problems. While quantum computers are not faster for everyday tasks like word processing, they are dramatically faster at specific mathematical problems that underpin modern cryptography.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

2.2. Shor's Algorithm and Public-Key Cryptography

In 1994, mathematician Peter Shor discovered a quantum algorithm that can efficiently solve two problems considered extremely hard for classical computers: factoring large numbers and computing discrete logarithms. These are precisely the foundations of the most widely deployed public-key cryptographic systems. RSA relies on the difficulty of factoring large numbers. ECDSA and EdDSA rely on the elliptic curve discrete logarithm problem. Diffie-Hellman and ECDH key exchanges also rely on discrete logarithm assumptions. A sufficiently powerful quantum computer running Shor's algorithm would break **all** of these systems, regardless of key size.

2.3. The "Harvest Now, Decrypt Later" Threat

For judicial systems, the threat timeline is particularly concerning because court records must remain verifiable for decades:

1. **Today:** An adversary records classically-signed judicial records.
2. **Future (2030–2040):** With CRQCs, the adversary forges new signatures under classical schemes.
3. **Impact:** Retroactive falsification of verdicts, evidence, and judicial reasoning.

The U.S. government has explicitly recognized this threat: National Security Memorandum 10 (NSM-10, May 2022) mandates federal agencies transition to PQ cryptography. CNSA 2.0 requires PQ algorithms by 2025 and exclusive use by 2033. Judicial records demand at least equivalent protection.

Why Post-Quantum Security Must Be Deployed Now

The key insight is that **the time to protect records is now, not when quantum computers arrive**. If a court verdict is signed today with a classical algorithm like ECDSA, and a quantum computer becomes available in 2035, then every verdict signed between now and 2035 becomes retroactively vulnerable to forgery. The only way to close this window is to begin using post-quantum signatures immediately.

2.4. Grover's Algorithm and Symmetric/Hash Security

Grover's algorithm (1996) provides a quadratic speedup for searching, effectively halving symmetric key strength. TRUST-Court mandates **AES-256** (128-bit PQ security) and **SHA-3-256** (128-bit PQ pre-image resistance) to maintain comfortable security margins.

3. Related Work

Several countries have taken steps toward digitizing their judicial systems, though none has yet implemented a comprehensive post-quantum secure framework.

Estonia pioneered with its e-Court system (2006), enabling electronic filing and case tracking, but relies on classical cryptographic signatures vulnerable to future quantum attacks. **Singapore's** eLitigation platform provides modern web-based court management with digital signature support, also without post-quantum primitives. **China** introduced blockchain-based evidence preservation in its Internet Courts starting in 2017, a significant step, but the underlying blockchain uses classical cryptography. The **European Union's** e-CODEX project enables cross-border judicial communication, and the eIDAS Regulation provides a legal framework for electronic signatures, but does not mandate post-quantum algorithms.

In the **United States**, PACER provides electronic access to federal court documents but lacks any cryptographic integrity—documents are simply PDF files on a server, with no way for citizens to verify authenticity mathematically. In **India**, the eCourts Mission Mode Project (Phase III, 2023) has digitized case filing and tracking across district courts, but does not provide tamper-evident records. Decentralized justice platforms such as Kleros and OpenLaw explore blockchain-based dispute resolution for private arbitration, but none employs post-quantum security.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

Legally, the eIDAS Regulation (EU), India's IT Act 2000 (Section 3A), and the US E-SIGN Act (2000) provide statutory foundations for digital signatures in judicial contexts. In **Ireland**, the Courts Service provides online case tracking and the courts.ie portal publishes selected judgments, but lacks cryptographic integrity guarantees. The Legal Aid Board and FLAC (Free Legal Advice Centres) assist citizens but operate with limited access to comprehensive precedent databases. Ireland benefits from the EU's eIDAS framework for electronic signatures and the Electronic Commerce Act 2000, providing a strong statutory foundation for digital court records.

None of the existing systems employ post-quantum cryptographic primitives, representing a critical gap that TRUST-Court is designed to fill.

4. Post-Quantum Cryptographic Primitives

This section introduces the cryptographic building blocks of TRUST-Court. For readers unfamiliar with cryptography, we provide plain-language explanations alongside technical specifications. The central idea is simple: every important action in the court system relies on mathematical operations that are believed to be impossible to reverse, even with a quantum computer.

Table 1 summarizes all cryptographic primitives.

Table 1. Complete Cryptographic Primitive Suite for TRUST-Court

Primitive	Algorithm	Purpose	PQ Sec.	Standard
PQ Signature	ML-DSA-65	Session & verdict signatures	NIST L3	FIPS 204
Archival Sig.	SLH-DSA-192f	Long-term verdict archival	NIST L3	FIPS 205
Classical Sig.	Ed25519	Hybrid backward compat.	128-bit	RFC 8032
PQ KEM	ML-KEM-768	Secure channel, key transport	NIST L3	FIPS 203
Classical KEM	X25519	Hybrid key exchange	128-bit	RFC 7748
Hash	SHA-3-256	Document hashing, Merkle trees	128-bit PQ	FIPS 202
Hash (Enhanced)	SHA-3-384	Certificate fingerprints	192-bit PQ	FIPS 202
Symmetric Enc.	AES-256-GCM	Data at rest and in transit	128-bit PQ	FIPS 197
Key Derivation	HKDF-SHA3-256	Session key derivation	128-bit PQ	RFC 5869
PRNG	CTR_DRBG-256	Nonce and key generation	128-bit PQ	SP 800-90A

4.1. ML-DSA-65: Primary Signature Scheme

What it does (plain language): ML-DSA is the primary digital signature algorithm. When a judge, lawyer, or party signs a court document, they create a mathematical "seal" that proves they approved it. If anyone changes even a single character after signing, the seal breaks and the tampering is detected.

Technical specification: ML-DSA (FIPS 204) is based on Module-LWE and Module-SIS over polynomial rings. ML-DSA-65 provides NIST Level 3 security with 1,952-byte public keys, 3,293-byte signatures, signing in 0.5 ms, and verification in 0.3 ms.

4.2. SLH-DSA-SHA2-192f: Archival Hash-Based Signatures

What it does (plain language): SLH-DSA is a backup signature used specifically for final verdicts. While ML-DSA relies on lattice mathematics, SLH-DSA relies *solely* on hash function security—the most battle-tested and conservative assumption in cryptography. Even if a breakthrough someday weakens lattice-based schemes, hash-based signatures would remain secure.

Technical specification: SLH-DSA (FIPS 205, based on SPHINCS+) relies **solely on hash function security**. Public keys are 48 bytes (remarkably small), but signatures are 35,664 bytes (large, yet acceptable for one-time verdict sealing). Signing takes approximately 15 ms and verification 1.5 ms.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

4.3. ML-KEM-768: Post-Quantum Key Encapsulation

What it does (plain language): ML-KEM enables two parties to establish a shared secret key over an insecure network, used in TRUST-Court to create encrypted communication channels for sensitive case information.

Technical specification: ML-KEM (FIPS 203) provides quantum-resistant key exchange with 1,184-byte public keys and 1,088-byte ciphertexts at NIST Level 3, achieving IND-CCA2 security under Module-LWE.

4.4. Hybrid Signature Construction

During the transition period, TRUST-Court employs **hybrid signatures** combining classical and post-quantum algorithms for defense in depth:

$$\sigma_{\text{hybrid}} = \sigma_{\text{Ed25519}} \parallel \sigma_{\text{ML-DSA-65}} \tag{1}$$

Verification requires **both** to be valid. For final verdicts, a triple hybrid adds SLH-DSA:

$$\sigma_{\text{verdict}} = \sigma_{\text{Ed25519}} \parallel \sigma_{\text{ML-DSA-65}} \parallel \sigma_{\text{SLH-DSA-192f}} \tag{2}$$

What this means for citizens: A verdict protected by a triple hybrid signature is secured by three completely independent mathematical assumptions. For it to be forged, an attacker would need to simultaneously break elliptic curve mathematics, lattice mathematics, and hash function security—a scenario cryptographers consider essentially impossible.

Post-Quantum Readiness Levels

1. **PQ-H (Hybrid):** Ed25519 + ML-DSA-65, X25519 + ML-KEM-768. *From Day 1.*
2. **PQ-F (Full):** ML-DSA-65 only, ML-KEM-768 only. *Target: Year 3.*
3. **PQ-A (Archival):** SLH-DSA added for all verdicts. *From Day 1 for verdicts.*

5. System Architecture

TRUST-Court is organized into five layers, each responsible for a specific aspect. Think of these layers like the floors of a building: each builds upon the one below it. Figure 1 presents the architecture.

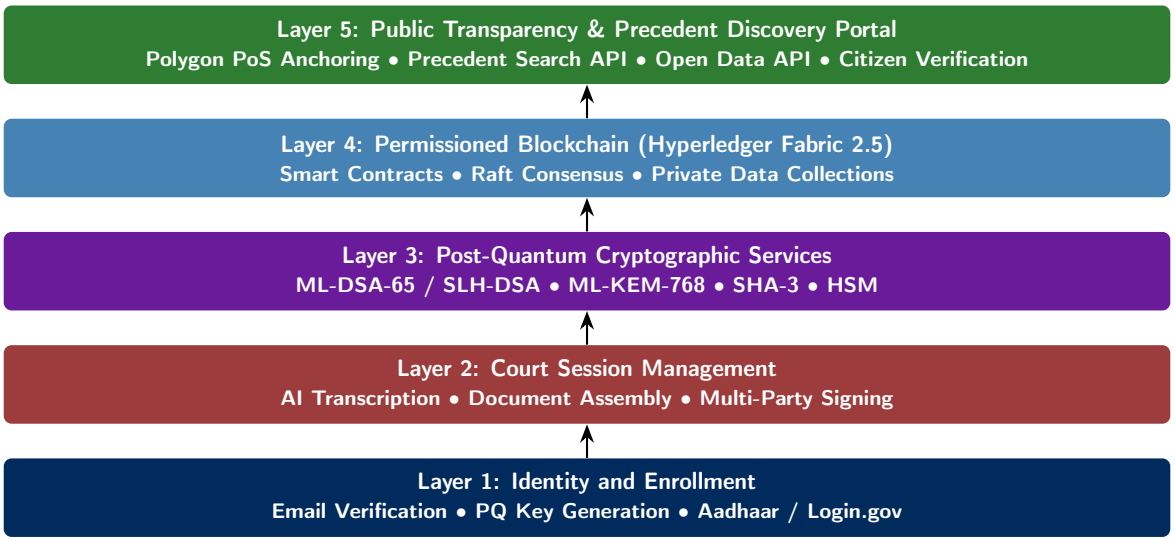

Figure 1. Five-layer architecture of TRUST-Court. Post-quantum cryptographic services (Layer 3) underpin all operations.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

5.1. Layer 1: Identity and Enrollment

Plain language: Before anyone can participate, they must prove who they are and receive digital credentials—similar to showing ID before entering a secure building, except the "ID" here is a set of cryptographic keys for signing documents securely.

Technical: Each participant registers via a government portal, undergoes identity verification (Login.gov IAL2 for USA; Aadhaar eKYC for India), and receives PQ key pairs generated in a FIPS 140-3 Level 3 HSM: ML-DSA-65 signing keys, Ed25519 hybrid keys, ML-KEM-768 encapsulation keys, and (for judges) SLH-DSA-SHA2-192f archival keys. An X.509v3 certificate with PQ extensions is issued.

5.2. Layer 2: Court Session Management

Plain language: During a hearing, everything said is captured by AI speech recognition, verified by a human operator, and assembled into a structured digital transcript. Every piece of evidence is "fingerprinted" using a hash function so any future tampering is detected instantly.

Technical: Real-time AI transcription with human verification, structured JSON document assembly with NTP-synchronized timestamps and speaker attribution, and SHA-3-256 evidence hashing.

5.3. Layer 3: PQ Cryptographic Services

Plain language: This is the security engine—every signature, encryption, and hash computation is performed here using post-quantum algorithms running inside tamper-proof hardware modules (HSMs).

Technical: HSM-backed ML-DSA-65 + Ed25519 hybrid signatures for sessions; triple hybrid (+ SLH-DSA) for verdicts; ML-KEM-768 hybrid key exchange for TLS channels; AES-256-GCM encryption; SHA-3-256/384 hashing.

5.4. Layer 4: Hyperledger Fabric

Plain language: Once a court record is signed, it is stored on a private blockchain operated by authorized judicial institutions. A blockchain is a distributed database where records are linked using cryptographic hashes, making it effectively impossible to alter a past record without detection.

Technical: Permissioned blockchain with PQ-enabled MSP, Raft consensus, chaincode for PQ signature verification, and private data collections for sealed records.

5.5. Layer 5: Public Transparency and Precedent Discovery

Plain language: A cryptographic hash of each published verdict is written to a public blockchain (Polygon), where anyone in the world can verify it. Citizens visit a transparency portal, enter a case number, and receive mathematical confirmation. Critically, this layer also provides a **Precedent Search API** that allows any person—lawyers, judges, citizens, researchers, and journalists—to search the entire corpus of published verdicts by legal issue, statute, keyword, or outcome. Every returned result can be cryptographically verified, and every citation carries a mathematical proof of authenticity (see Section 14 for full details).

Technical: SHA-3-256 verdict hashes anchored to Polygon PoS. Citizen verification portal, Open Data API, and Precedent Search API (full-text + structured metadata) for published records. Elasticsearch-based indexing of verdict text, legal provisions, precedent citations, and outcome classifications.

6. Enrollment Protocol

The enrollment process ensures that every participant has been properly identified and received the cryptographic keys necessary to participate. Figure 2 shows the flow.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

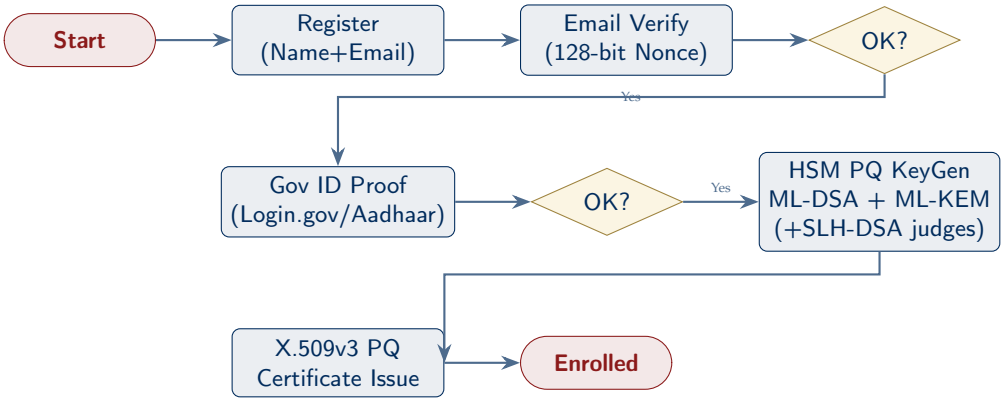

Figure 2. Enrollment protocol: email verification, government ID proofing, PQ key generation in HSM, and X.509v3 certificate issuance.

7. Court Session Recording and Signing Protocol

The court session protocol defines how a hearing is recorded, verified, and signed. It has four phases (Figure 3).

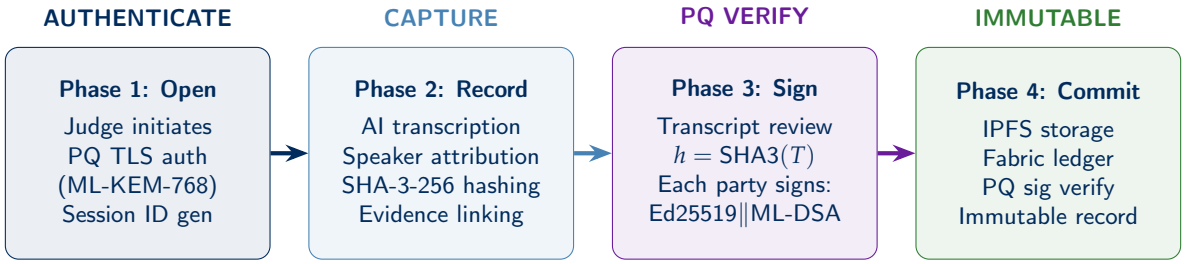

Figure 3. Four-phase court session protocol with post-quantum cryptography at every stage.

At session end, each participant i signs:

$$\sigma_i = \text{Ed25519.Sign}(sk_{i,\text{Ed}}, h_T) \parallel \text{ML-DSA-65.Sign}(sk_{i,\text{ML}}, h_T) \tag{3}$$

where $h_T = \text{SHA-3-256}(T)$. The record $R = \{T, \text{metadata}, h_T, \{\sigma_i\}, \{\text{Cert}_i\}\}$ is stored on IPFS and committed to Fabric after chaincode verifies all signatures.

Algorithm 1 Post-Quantum Court Session Signing Protocol

Require: Transcript T, Participants $\mathcal{P} = \{P_1, \ldots, P_n\}$ with $(sk_{i,\text{Ed}}, sk_{i,\text{ML}})$
Ensure: Signed record R on blockchain
1: $h_T \leftarrow \text{SHA-3-256}(T)$
2: **for** each $P_i \in \mathcal{P}$ **in parallel do**
3: $\quad \sigma_i \leftarrow \text{Ed25519.Sign}(sk_{i,\text{Ed}}, h_T) \| \text{ML-DSA.Sign}(sk_{i,\text{ML}}, h_T)$
4: **end for**
5: $\text{CID}_T \leftarrow \text{IPFS.Store}(T)$
6: $R \leftarrow \{\texttt{SID}, h_T, \text{CID}_T, \{(pk_i, \sigma_i)\}_{i=1}^{n}\}$
7: Fabric.SubmitTransaction(R) {chaincode verifies all PQ sigs}

8. Verdict Issuance and Public Publication

The verdict document V receives the highest cryptographic protection: a **triple hybrid PQ signature** (Eq. 2). Figure 4 shows the publication flow.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

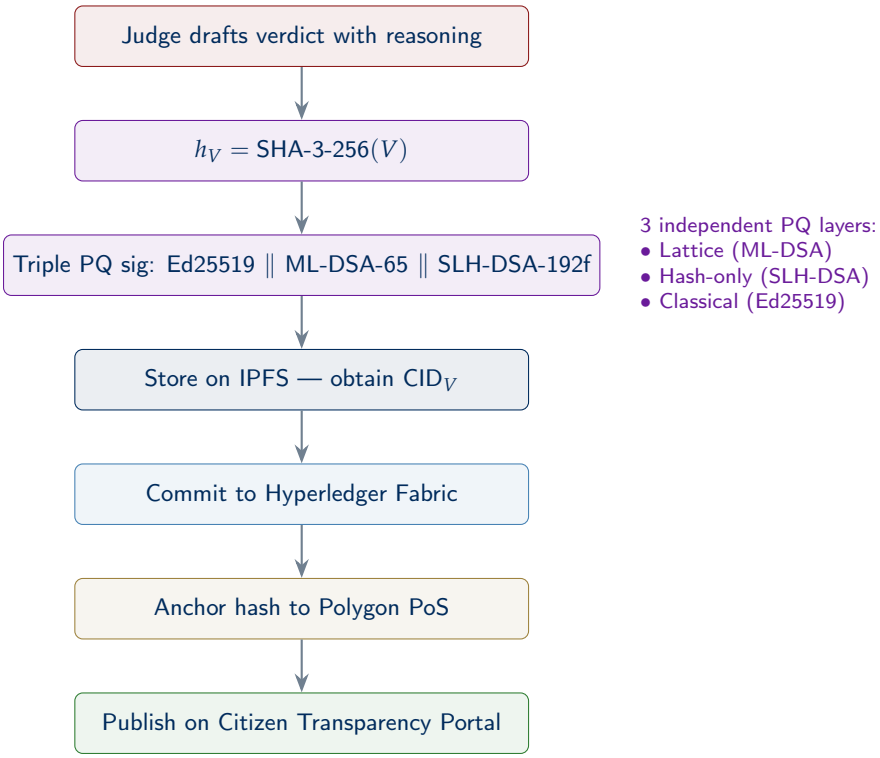

Figure 4. Verdict publication protocol with triple hybrid post-quantum signatures.

9. Blockchain Architecture

TRUST-Court uses a **dual-chain architecture** combining two blockchain types (Figure 5).

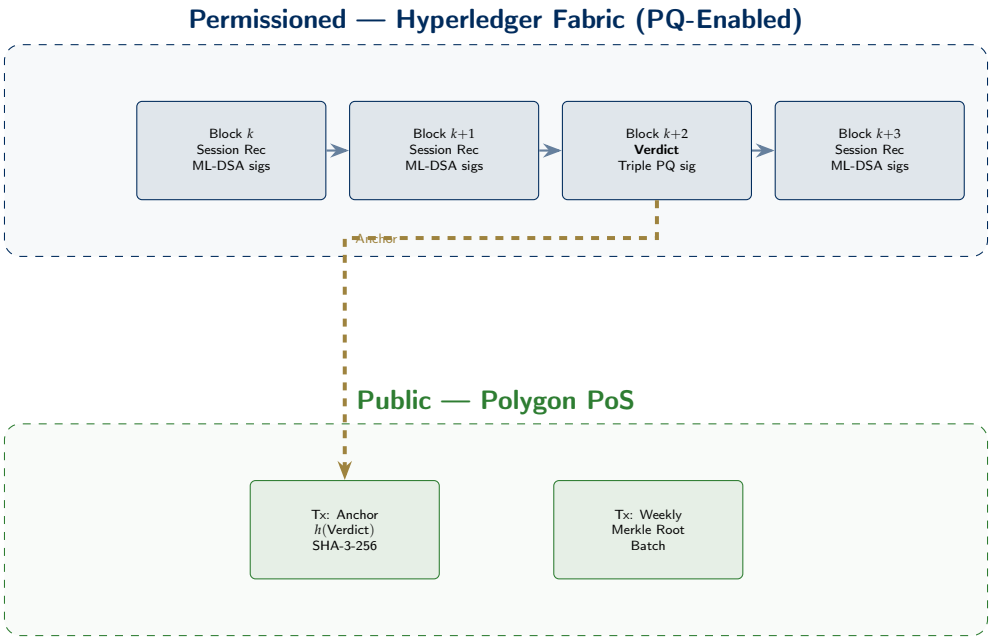

Figure 5. Dual-chain architecture: Hyperledger Fabric (permissioned, PQ signatures) with Polygon PoS (public anchoring).

US topology: 13 circuit organizations + SCOTUS, 94 district court peers, 5-node Raft orderer. **India:** Supreme Court + 25 High Courts + NIC, ∼700 district peers (phased), 7-node Raft.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

10. Case Study 1: US Patent Litigation — *Smith v. TechCorp*

This section presents a detailed walkthrough of a multi-session patent infringement proceeding in a U.S. federal court, demonstrating how TRUST-Court handles complex civil litigation—from party enrollment through twelve hearing sessions to a final, publicly verifiable verdict.

Key Insight

Scenario: Independent inventor John Smith alleges that TechCorp Inc., a Silicon Valley technology company, infringed his software patent (US10,XXX,XXX) covering a novel data compression algorithm. The case is filed in the U.S. District Court, Northern District of California, San Jose Division. Damages sought: $4.2 million in lost licensing royalties plus a permanent injunction.

10.1. Step 1: Party Enrollment

Before the case can proceed in TRUST-Court, all participants must be enrolled with verified digital identities and post-quantum cryptographic keys.

1. **Plaintiff — John Smith** (`jsmith@email.com`): Mr. Smith registers on the federal judiciary's TRUST-Court portal. He verifies his email via a 128-bit cryptographic nonce, then completes identity proofing through Login.gov at Identity Assurance Level 2 (IAL2), which requires document verification and a selfie match. His PQ key suite is generated in an HSM: ML-DSA-65 + Ed25519 signing keys, ML-KEM-768 encapsulation keys. An X.509v3 PQ certificate is issued with role: `Plaintiff`.
2. **Plaintiff's Attorney — Sarah Johnson** (`sjohnson@lawfirm.com`): Ms. Johnson is already enrolled as an active member of the California Bar with a TRUST-Court PQ certificate (role: `Attorney`). Her keys were generated during her initial enrollment and are stored in her law firm's FIPS 140-3 Level 3 HSM.
3. **Defense Counsel — Mark Davis** (`mdavis@techcorplegal.com`): Mr. Davis, representing TechCorp, completes the same enrollment process. His certificate includes his California Bar number and role: `Attorney`.
4. **Presiding Judge — Hon. Patricia Chen**: Judge Chen is enrolled with the full judicial PQ key suite, which includes the standard ML-DSA-65 + Ed25519 + ML-KEM-768 keys *plus* an SLH-DSA-SHA2-192f archival key. This additional key is reserved for judges and is used exclusively for verdict sealing, providing the most conservative cryptographic protection for final judicial orders.

Why enrollment matters here: Every person who participates in the trial receives unique cryptographic keys tied to their verified real-world identity. This means every digital signature can be traced to a specific, verified individual. No one can later claim "I didn't sign that" or "someone else signed on my behalf"—the mathematics make impersonation impossible.

10.2. Step 2: Case Filing and Evidence Submission

1. Ms. Johnson files the complaint digitally via the TRUST-Court e-filing system: `NDCA-SJ-2027-CV-01847`. The filing is digitally signed with her hybrid PQ keys:

$$\sigma_{\text{filing}} = \text{Ed25519.Sign}(sk_{\text{Johnson,Ed}}, h_f) \parallel \text{ML-DSA.Sign}(sk_{\text{Johnson,ML}}, h_f) \tag{4}$$

   where $h_f = \text{SHA-3-256}(\text{complaint\_document})$.
2. Patent documents (Exhibit P-1), source code comparison reports (Exhibit P-2), licensing history records (Exhibit P-3), and expert analysis (Exhibit P-4) are each hashed with SHA-3-256 and stored on IPFS with their Content Identifiers (CIDs) linked to the case record.
3. TechCorp's answer and counterclaims are similarly filed and PQ-signed by Mr. Davis. Prior art references (Exhibit D-1 through D-6) are hashed and linked.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

4. All filings are committed to the Hyperledger Fabric blockchain (Northern District of California channel), creating an immutable, timestamped record of every document submitted.

10.3. Step 3: Court Sessions 1–12

The trial spans twelve court sessions over four months. Each session follows the four-phase protocol (Open, Record, Sign, Commit).

10.3.1. 3a. Representative Session: Expert Testimony (Session 7)

- Judge Chen opens Session `SID-007` via the TRUST-Court court terminal.
- All 4 participants authenticate via PQ TLS (X25519 + ML-KEM-768 hybrid handshake).
- AI transcription captures all testimony in real time with speaker attribution and NTP-synchronized timestamps.

Court Transcript Excerpt — Session SID-007 (Expert Testimony)

[2:01 PM] Judge Chen: "The court will now hear expert testimony regarding the technical comparison of the patented algorithm and TechCorp's implementation. Ms. Johnson, please call your expert."
[2:03 PM] Atty. Johnson: "Your Honor, the plaintiff calls Dr. Robert Kim, Professor of Computer Science at Stanford University, as an expert witness in software algorithms and data compression. Dr. Kim's report has been submitted as Exhibit P-4, SHA-3-256 hashed and verified on-chain."
[2:05 PM] Dr. Kim: "I conducted a line-by-line comparison of the patented algorithm described in Claims 1 through 7 of US10,XXX,XXX with TechCorp's `CompressMax` module, version 3.2. My analysis found that TechCorp's implementation uses the same novel three-stage pipeline described in the patent: adaptive dictionary construction, entropy-weighted partitioning, and recursive block merging. The implementation differences are cosmetic—variable renaming and language translation from C to Rust—but the algorithmic structure is identical."
[2:12 PM] Atty. Davis: "Dr. Kim, isn't it true that the three-stage pipeline concept existed in academic literature before Mr. Smith's patent filing?"
[2:14 PM] Dr. Kim: "The individual stages have prior art. However, the specific combination—particularly the entropy-weighted partitioning feeding into recursive block merging with the adaptive dictionary—is novel. I reviewed the six prior art references submitted by the defense and none teaches this specific combination."
[2:18 PM] Judge Chen: "The court notes that Exhibit P-4 is SHA-3-256 verified and will be considered alongside the prior art exhibits. Are there further questions?"
[2:20 PM] Atty. Davis: "No further questions, Your Honor."
[2:21 PM] Judge Chen: "The expert testimony is concluded. We will proceed to closing arguments in Session 12."

10.3.2. 3b. Multi-Party PQ Signing of Each Session

At the conclusion of each session, the transcript signing proceeds identically:

1. The complete transcript T is displayed for all 4 participants to review on courtroom terminals.
2. Any corrections are proposed, reviewed, and appended as amendments.
3. Final hash: $h_T = \text{SHA-3-256}(T)$.
4. Each participant signs with hybrid PQ keys:

$$\sigma_i = \text{Ed25519.Sign}(sk_{i,\text{Ed}}, h_T) \parallel \text{ML-DSA-65.Sign}(sk_{i,\text{ML}}, h_T) \quad \text{(3,357 bytes each)} \tag{5}$$

5. Total signature data per session: $4 \times 3{,}357 = 13{,}428$ bytes ($\approx$13.1 KB).
6. Transcript stored on IPFS; record committed to Fabric after chaincode verifies all 4 PQ signatures.

Over 12 sessions, the case accumulates $12 \times 13{,}428 = 161{,}136$ bytes ($\approx$157 KB) of signature data—efficiently batched using Merkle-tree signature batching (Section 16) into a single 32-byte on-chain root.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

10.4. Step 4: Verdict

After closing arguments in Session 12, Judge Chen delivers the verdict.

Verdict — Case NDCA-SJ-2027-CV-01847

Findings of Fact:

1. Plaintiff John Smith is the sole inventor and assignee of U.S. Patent No. US10,XXX,XXX, filed on 14 March 2022 and granted on 7 September 2023.
2. Defendant TechCorp Inc. released its `CompressMax` software module (version 3.2) on 15 January 2025, which implements a data compression algorithm.
3. Expert testimony (Exhibit P-4, Dr. Robert Kim) established that TechCorp's implementation replicates the novel three-stage pipeline described in Claims 1–7 of the patent.
4. The defense's prior art references (Exhibits D-1 through D-6) establish the existence of individual algorithmic stages but do not teach the specific combination claimed in the patent.

Legal Reasoning:

Under the claim construction framework established in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005), the court construes the claims of US10,XXX,XXX in light of the specification and prosecution history. The court finds that TechCorp's `CompressMax` module infringes Claims 1, 3, 5, 6, and 7 under the doctrine of equivalents. The algorithmic structure is functionally identical, and the implementation differences (language translation and variable renaming) do not constitute a meaningful distinction under *Graver Tank & Mfg. Co. v. Linde Air Products Co.*, 339 U.S. 605 (1950).

Regarding damages, the court applies a reasonable royalty analysis under 35 U.S.C. §284. Based on comparable licensing agreements in the data compression industry (Exhibits P-5 and P-6) and TechCorp's revenue attributable to `CompressMax`, the court awards damages of **$4,200,000**.

Order:

1. TechCorp Inc. is found to have infringed Claims 1, 3, 5, 6, and 7 of U.S. Patent No. US10,XXX,XXX.
2. A **permanent injunction** is issued against TechCorp's continued use, sale, or distribution of the infringing `CompressMax` module.
3. TechCorp shall pay damages of **$4,200,000** to the plaintiff within 60 days.
4. Each party shall bear its own costs.

Judge's Comment:

"This case underscores the importance of thorough prior art searches before product development. The court notes that TRUST-Court's blockchain-verified evidence chain eliminated the typical disputes over document authenticity and exhibit provenance that often prolong patent litigation. All twelve session transcripts were PQ-signed by all parties, leaving no room for transcript disputes on appeal."

10.5. Step 5: PQ Cryptographic Sealing of Verdict

1. Judge Chen's verdict document V is finalized in the TRUST-Court system.
2. Hash computed: $h_V = \text{SHA-3-256}(V)$ — 32 bytes.
3. **Triple hybrid archival signature:**

$$\begin{aligned}\sigma_{\text{verdict}} = {} & \text{Ed25519.Sign}(sk_{\text{Chen,Ed}}, h_V) \quad \text{(64 bytes)} \\ & \| \ \text{ML-DSA-65.Sign}(sk_{\text{Chen,ML}}, h_V) \quad \text{(3,293 bytes)} \\ & \| \ \text{SLH-DSA.Sign}(sk_{\text{Chen,SLH}}, h_V) \quad \text{(35,664 bytes)}\end{aligned} \tag{6}$$

   Total signature: 39,021 bytes (≈38 KB).
4. Verdict stored on IPFS: $\text{CID}_V =$ `bafybei...`
5. Committed to Fabric (Northern District of California channel).
6. SHA-3-256 hash anchored to Polygon PoS: transaction hash `0x3e8b...`
7. Published on the federal judiciary's transparency portal.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

10.6. Step 6: Public Verification and Appeal Implications

Any person can verify this verdict:

1. Visit the federal transparency portal at `transparency.uscourts.gov/verify`.
2. Enter case number `NDCA-SJ-2027-CV-01847` or scan the QR code on the verdict document.
3. The portal retrieves the verdict from IPFS, recomputes SHA-3-256, and verifies the on-chain Polygon anchor.
4. All three components of Judge Chen's triple PQ signature are verified against her published X.509v3 certificate.
5. A green checkmark confirms: "Verdict integrity verified. All post-quantum signatures valid."

Appeal implications: If TechCorp appeals to the Federal Circuit, the appellate court can independently verify the complete trial record—all twelve session transcripts and the verdict—using the same cryptographic verification process. Because every transcript was PQ-signed by all four participants, there is no possibility of transcript disputes on appeal. The mathematical record is definitive.

How others discover this verdict: Beyond the parties themselves, the general public learns about this verdict through multiple channels (see Section 14): it appears automatically on the public verdict feed at `transparency.uscourts.gov/feed`, is discoverable via keyword searches such as "data compression patent infringement Northern District California," is reported by legal news outlets with embedded verification widgets, and is indexed in the Precedent Search API for any future litigant to cite. A patent attorney in Texas preparing a similar infringement case can find this ruling without knowing its case number—a simple search for "software patent + doctrine of equivalents + permanent injunction" returns it alongside all comparable verdicts.

11. Case Study 2: India Criminal Case — *State of Maharashtra v. Rajesh Kumar*

This section presents a detailed walkthrough of a cybercrime prosecution in India, demonstrating how TRUST-Court handles criminal proceedings with Aadhaar-based enrollment, bilingual Hindi/Marathi transcription, digital forensic evidence, and the full PQ signature lifecycle from first hearing to sentencing.

Key Insight

Scenario: Between March and August 2026, Mr. Rajesh Kumar allegedly operated a phishing scheme that impersonated a major Indian bank's website, stealing login credentials and transferring funds from 47 victim accounts totaling INR 38,00,000 (approximately $45,000). The case is prosecuted under Section 66C of the Information Technology Act, 2000 (identity theft) and Section 420 of the Indian Penal Code (cheating). The trial takes place at the Sessions Court, Mumbai.

11.1. Step 1: Party Enrollment via Aadhaar eKYC

All participants enroll in TRUST-Court using India's Aadhaar identity system, which provides biometric verification for over 1.3 billion citizens.

1. **Public Prosecutor — Anita Desai**: Ms. Desai registers on `ecourts.gov.in` and completes Aadhaar eKYC verification (fingerprint + OTP). Her PQ key suite is generated: ML-DSA-65 + Ed25519 + ML-KEM-768. An X.509v3 PQ certificate is issued with role: `Public Prosecutor`, linked to her Maharashtra Bar Council registration number.
2. **Accused — Rajesh Kumar**: Mr. Kumar enrolls at a court kiosk located in the Sessions Court lobby. Because he is in judicial custody, a court officer supervises the enrollment. Aadhaar eKYC verification is completed via iris scan (as his fingerprints are already on file with the police). His PQ key suite is generated and stored in the court kiosk's HSM. His certificate role is `Accused`.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

3. **Defense Advocate — Suresh Patel**: Mr. Patel is already enrolled with an active PQ certificate through his prior participation in other TRUST-Court proceedings. His keys reside in his law office's HSM.
4. **Presiding Judge — Hon. Meera Rao**: Judge Rao holds the full judicial PQ key suite including SLH-DSA-SHA2-192f archival keys. Her certificate is issued by the Supreme Court of India's PQ Root Certificate Authority (ML-DSA-87).

Aadhaar enrollment advantage: India's Aadhaar system provides a unique advantage for TRUST-Court deployment. Unlike the US, where identity proofing requires document verification through Login.gov, Aadhaar enables biometric identity verification in seconds—even at a court kiosk. This makes enrollment accessible even in rural district courts.

11.2. Step 2: Case Filing and Digital Evidence Linking

1. The First Information Report (FIR) from the Cyber Crime Cell, Mumbai Police, is digitally signed by the investigating officer and committed to the Hyperledger Fabric blockchain (Maharashtra Police channel). Its IPFS CID is linked to the case.
2. Case filed digitally: `SC-Mumbai-2026-Crim-04291`.
3. Digital forensic evidence is submitted and hash-linked:
   - Exhibit P-1: Server logs from the phishing domain (SHA-3-256 hashed, 32 bytes fingerprint)
   - Exhibit P-2: Email headers showing phishing campaign distribution
   - Exhibit P-3: Bank transaction records showing unauthorized transfers from 47 accounts
   - Exhibit P-4: IP address trace report linking activity to the accused's residence
   - Exhibit P-5: Forensic image of the accused's laptop (hash of disk image stored; full image on IPFS)
4. Each exhibit is PQ-signed by the investigating officer and the forensic examiner, then committed to Fabric. This creates an unbreakable chain of custody—no one can later allege that evidence was tampered with after seizure.

11.3. Step 3: Court Sessions — Trial Proceedings

The trial spans six sessions over two months, conducted bilingually in Hindi and Marathi.

11.3.1. 3a. Session Initialization

- Judge Rao opens Session `SID-001` via the TRUST-Court terminal at Sessions Court, Mumbai.
- All participants authenticate via PQ TLS using X.509v3 PQ certificates.
- The AI transcription system is configured for bilingual Hindi/Marathi mode, with each utterance tagged with the language detected.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

11.3.2. 3b. Representative Session: Digital Forensic Evidence (Session 3)

Court Transcript Excerpt — Session SID-003 (Forensic Evidence)

[11:02 AM] Judge Rao: "*Yeh adalat ab Case No. SC-Mumbai-2026-Crim-04291 mein sunwai karti hai.* The prosecution may present digital forensic evidence." [Hindi/English]
[11:05 AM] PP Desai: "Your Honor, I call Inspector Amit Joshi from the Cyber Crime Cell as the prosecution's forensic witness. Inspector Joshi supervised the seizure and forensic analysis of the accused's electronic devices."
[11:07 AM] Inspector Joshi: "Your Honor, on 12 September 2026, we executed a search warrant at the accused's residence in Andheri West. We seized one laptop, two mobile phones, and one external hard drive. All devices were forensically imaged in the presence of two independent witnesses, and the disk images were SHA-3-256 hashed immediately. The hash values were recorded in the seizure panchnama and signed digitally by both witnesses. I submit the forensic image hashes as Exhibit P-5."
[11:12 AM] Judge Rao: "Exhibit P-5 is admitted. The court notes the SHA-3-256 hashes are verified against the on-chain record. *Kya hash values match karte hain?*" [Hindi]
[11:13 AM] Court Technical Officer: "*Ji haan, Your Honor.* All five hash values match the blockchain-recorded values from the date of seizure. No tampering detected." [Hindi/English]
[11:15 AM] Inspector Joshi: "Analysis of the laptop revealed a complete phishing toolkit, including cloned bank login pages, a database of 47 stolen credentials, and scripts for automated fund transfers. The IP addresses used for phishing domain registration trace back to the accused's broadband connection, as documented in Exhibit P-4."
[11:20 AM] Adv. Patel: "Inspector Joshi, *kya aapne verify kiya ki laptop sirf mere client ne use kiya tha?* Did you verify that only my client used the laptop?" [Hindi/English]
[11:22 AM] Inspector Joshi: "The laptop was password-protected with the accused's personal credentials. Browser history and login timestamps correlate with the accused's presence at the residence, as confirmed by mobile phone location data. There is no evidence of third-party access."
[11:25 AM] Judge Rao: "*Agla witness bulayein.* The prosecution may call the next witness."

11.3.3. 3c. Multi-Party PQ Signing of Each Session

1. After each session, the bilingual transcript T is displayed on courtroom terminals for all 4 participants.
2. Language tags are verified—participants confirm that Hindi and Marathi portions are accurately attributed.
3. Final hash: $h_T = \text{SHA-3-256}(T)$.
4. Each participant signs:

$$\sigma_i = \text{Ed25519.Sign}(sk_{i,\text{Ed}}, h_T) \parallel \text{ML-DSA-65.Sign}(sk_{i,\text{ML}}, h_T) \quad \text{(3,357 bytes each)} \tag{7}$$

5. Total per session: $4 \times 3{,}357 = 13{,}428$ bytes. Over 6 sessions: ≈78.6 KB of signature data.
6. All transcripts stored on IPFS and committed to Fabric (Maharashtra Judiciary channel).

11.4. Step 4: Verdict

After hearing all evidence and arguments across six sessions, Judge Rao delivers the verdict.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

Verdict — Case SC-Mumbai-2026-Crim-04291

Findings of Fact:

1. The accused, Mr. Rajesh Kumar, resident of Andheri West, Mumbai, operated a phishing scheme between March and August 2026 impersonating a major Indian bank.
2. Digital forensic evidence (Exhibits P-1 through P-5) established that the phishing toolkit, stolen credentials, and fund transfer scripts were found on the accused's personal laptop, secured with his credentials.
3. Bank transaction records (Exhibit P-3) confirm unauthorized transfers totaling INR 38,00,000 from 47 victim accounts to mule accounts controlled by the accused.
4. IP address trace evidence (Exhibit P-4) links the phishing domain to the accused's broadband connection.
5. The defense failed to establish that any third party had access to the accused's devices or accounts.

Legal Reasoning:

Section 66C of the Information Technology Act, 2000 penalizes whoever fraudulently or dishonestly makes use of the electronic signature, password, or any other unique identification feature of any other person. The evidence establishes beyond reasonable doubt that the accused created and operated a phishing infrastructure designed to steal banking credentials.

Section 420 of the Indian Penal Code punishes cheating and dishonestly inducing delivery of property. The unauthorized fund transfers totaling INR 38,00,000 from victims' accounts constitute cheating under this provision.

The court notes that the integrity of all digital forensic evidence was verified through TRUST-Court's blockchain-anchored SHA-3-256 hashes, eliminating any possibility of evidence tampering between seizure and trial—a common defense challenge in cybercrime cases.

Order:

1. The accused is found **guilty** under Section 66C of the IT Act, 2000 and Section 420 of the IPC.
2. Sentence: **3 years rigorous imprisonment**.
3. Fine: **INR 2,00,000**, of which INR 1,50,000 shall be directed toward victim compensation.
4. The accused's seized electronic devices shall be forfeited to the State.

Judge's Comment:

"*Digital identity theft ek gambhir aparadh hai jo logon ki bachat aur vishwas ko khatam karta hai.* Digital identity theft is a grave offense that destroys people's savings and trust. This court recommends that banking institutions implement stronger multi-factor authentication and that law enforcement agencies establish dedicated cyber forensic units in every district. The court further notes that TRUST-Court's tamper-evident evidence chain was instrumental in establishing the integrity of digital forensic evidence, which is often challenged in cybercrime proceedings. *Is faislay ko Hindi aur English dono mein prakashit kiya jaye.*"

11.5. Step 5: PQ Cryptographic Sealing of Verdict

1. Judge Rao's verdict document V is finalized in TRUST-Court.
2. Hash computed: $h_V = \text{SHA-3-256}(V)$ — 32 bytes.
3. **Triple hybrid archival signature:**

$$\begin{aligned}\sigma_{\text{verdict}} = {} & \text{Ed25519.Sign}(sk_{\text{Rao,Ed}}, h_V) \quad \text{(64 bytes)} \\ & \| \ \text{ML-DSA-65.Sign}(sk_{\text{Rao,ML}}, h_V) \quad \text{(3,293 bytes)} \\ & \| \ \text{SLH-DSA.Sign}(sk_{\text{Rao,SLH}}, h_V) \quad \text{(35,664 bytes)}\end{aligned} \tag{8}$$

   Total signature: 39,021 bytes (≈38 KB).
4. Verdict stored on IPFS: $\text{CID}_V =$ `bafybei...`.
5. Committed to Fabric (Maharashtra Judiciary channel).
6. SHA-3-256 hash anchored to Polygon PoS.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

7. Published bilingually on `transparency.ecourts.gov.in` in both English and Hindi.

11.6. Step 6: Public Verification and Victim Notification

1. Any citizen can verify the verdict on `transparency.ecourts.gov.in/verify` by entering case number `SC-Mumbai-2026-Crim-04291`.
2. The 47 victims are automatically notified via the TRUST-Court system that the verdict has been published and can be independently verified.
3. Victims eligible for compensation (INR 1,50,000 from the fine) can verify the order's authenticity before approaching the court for disbursement.

Multilingual significance: India has 22 scheduled languages. This case demonstrates TRUST-Court's ability to handle bilingual proceedings (Hindi/Marathi testimony with English legal citations), publish verdicts in multiple languages, and maintain a single cryptographically unified record. The underlying hash and signatures cover the complete multilingual document, ensuring that translations cannot diverge from the original without detection.

How others discover this verdict: The 47 victims are notified directly (Channel 3), but the broader public discovers this verdict through the real-time verdict feed filtered by "Sessions Court Mumbai + IT Act" (Channel 1), keyword searches such as "phishing identity theft bank conviction Mumbai" (Channel 2), news media reports with embedded verification widgets (Channel 6), and legal aid clinics advising cybercrime victims (Channel 7). A prosecutor in Delhi preparing a similar case can search "Section 66C + phishing + conviction + sentencing" and find this ruling with its complete reasoning, outcome, and one-click verification link—all without knowing the case number in advance (see Section 14 for the full discovery framework).

12. Case Study 3: Traffic Offence in Ireland — *DPP v. Seán O'Brien*

This section presents a detailed, step-by-step walkthrough of a common traffic offence case in Ireland, demonstrating how TRUST-Court handles everyday judicial proceedings within the Irish legal framework—from the moment a Garda issues a Fixed Charge Notice through to the final digitally-signed District Court verdict.

Key Insight

Scenario: On 15 January 2027, Garda Sergeant Aoife Brennan of the Cork City Division, An Garda Síochána, stops Mr. Seán O'Brien on the South Link Road, Cork, for driving with an expired driving licence. Under Section 38 of the Road Traffic Act 1961 (as amended), it is an offence to drive without a valid driving licence. A Fixed Charge Notice (FCN) is issued with a fine of €80 and 2 penalty points. Mr. O'Brien contests the charge, and the case proceeds to Cork District Court.

12.1. Step 1: Incident and Digital Fixed Charge Notice Issuance

1. Garda Sergeant Aoife Brennan uses the TRUST-Court-integrated Garda enforcement app on her government-issued mobile device.
2. She authenticates using her enrolled PQ digital identity (MyGovID-verified, ML-DSA-65 certificate issued by the Courts Service of Ireland PQ Certificate Authority).
3. The app captures: date/time (NTP-synchronized), GPS location (South Link Road, Cork, 51.8891°N, 8.4756°W), vehicle registration number (211-C-4567), and the offence (driving without valid licence, Section 38, Road Traffic Act 1961).
4. Garda Brennan digitally signs the electronic Fixed Charge Notice (e-FCN):

$$\sigma_{\text{FCN}} = \text{Ed25519.Sign}(sk_{\text{Brennan,Ed}}, h_f) \parallel \text{ML-DSA.Sign}(sk_{\text{Brennan,ML}}, h_f) \tag{9}$$

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

where h_f = SHA-3-256(FCN_data).

5. The signed e-FCN is committed to the Hyperledger Fabric network (An Garda Síochána — Courts Service channel).
6. Mr. O'Brien receives the e-FCN via post and email with a QR code linking to the blockchain record. Under the Road Traffic Act 2002 (as amended), he has 28 days to pay €80 (increasing to €120 after 28 days), or allow the matter to proceed to District Court.

12.2. Step 2: Contestation and Case Filing

1. Mr. O'Brien believes his licence was valid at the time of the stop. He had applied to renew his driving licence through the NDLS (National Driver Licence Service) online portal at `ndls.ie` on 20 December 2026, but the renewed licence card had not yet arrived by post. His old licence card showed an expiry date of 31 December 2026.
2. He does not pay the Fixed Charge Notice within the 56-day period. A summons is issued to appear at Cork District Court.
3. Mr. O'Brien registers on the TRUST-Court portal at `courts.ie/trust-court`, verifies his identity via MyGovID (the Irish government's digital identity service, backed by the Public Services Card), and receives his PQ key suite (ML-DSA-65 + Ed25519 + ML-KEM-768).
4. His solicitor, Ms. Ciara Fitzpatrick, is already enrolled with an active PQ certificate (role: `Solicitor`, Law Society of Ireland registration number linked).
5. A case is filed digitally: `DC-Cork-2027-Traffic-01193`. The e-FCN's IPFS CID and blockchain transaction ID are linked as the primary prosecution evidence.
6. Judge Brendan McCarthy is assigned to hear the case at Cork District Court. He is enrolled with the full judicial PQ key suite including SLH-DSA archival keys, issued by the Courts Service of Ireland PQ Root Certificate Authority.

12.3. Step 3: Court Session — Hearing

The hearing is conducted at Cork District Court, Washington Street, Cork, on 12 March 2027.

12.3.1. 3a. Session Initialization

- Judge McCarthy opens Session `SID-001` via the TRUST-Court court terminal.
- All participants authenticate via PQ TLS (X25519 + ML-KEM-768 hybrid handshake) using their X.509v3 PQ certificates.
- Participants: Judge McCarthy (Judge), Garda Sgt. Brennan (Prosecution Witness), Mr. O'Brien (Defendant), Ms. Fitzpatrick (Defense Solicitor), and the State Solicitor Mr. Declan Murphy representing the Director of Public Prosecutions.

12.3.2. 3b. Court Proceedings — Transcribed in Real Time

The following is a summary of the digitally transcribed proceedings (each utterance is timestamped and speaker-attributed):

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

Court Transcript Summary — Session SID-001

[10:32 AM] Judge McCarthy: "This court is now in session for Case No. DC-Cork-2027-Traffic-01193, *DPP v. Seán O'Brien*, under Section 38 of the Road Traffic Act 1961. The prosecution may present its case."
[10:34 AM] State Sol. Murphy: "Judge, on 15 January 2027, Garda Sergeant Aoife Brennan of the Cork City Division stopped the defendant on the South Link Road while driving vehicle 211-C-4567. The defendant produced a driving licence that had expired on 31 December 2026. A Fixed Charge Notice was issued and digitally signed on the spot. I submit the blockchain-verified e-FCN as Exhibit P-1."
[10:36 AM] Judge McCarthy: "Exhibit P-1 is admitted. The court notes the Fixed Charge Notice bears a valid ML-DSA-65 digital signature from Garda Brennan, verified on-chain. Garda Brennan, please provide your evidence."
[10:38 AM] Garda Brennan: "Judge, I stopped the defendant during a routine checkpoint on the South Link Road. Upon requesting his driving licence, he produced a licence card showing an expiry date of 31 December 2026. As the licence was expired, I issued a Fixed Charge Notice for driving without a valid driving licence under Section 38 of the Road Traffic Act. I signed the notice digitally on my Garda-issued device."
[10:42 AM] Judge McCarthy: "Ms. Fitzpatrick, the defence may cross-examine."
[10:43 AM] Sol. Fitzpatrick: "Garda Brennan, did you check the NDLS database to verify my client's licence status at the time of the stop?"
[10:44 AM] Garda Brennan: "I inspected the physical licence card, which showed the expiry date of 31 December 2026. I did not check the NDLS online system at that point."
[10:46 AM] Sol. Fitzpatrick: "Judge, I submit Exhibit D-1: a confirmation email from the NDLS dated 22 December 2026, acknowledging receipt of my client's online renewal application. I further submit Exhibit D-2: a record from the NDLS showing that the renewal was processed and approved on 3 January 2027, and the new licence card was dispatched on 8 January 2027 but had not yet been delivered by An Post at the time of the stop on 15 January 2027. I also submit Exhibit D-3: the An Post tracking record showing the licence card was delivered on 18 January 2027—three days after the stop."
[10:48 AM] Judge McCarthy: "Exhibits D-1, D-2, and D-3 are admitted. The court notes all three are SHA-3-256 hashed and linked to this session record."
[10:50 AM] Mr. O'Brien: "Judge, I applied to renew my licence well before the expiry date. The NDLS approved the renewal before I was stopped. The only reason I couldn't produce a valid licence card was the postal delay. I was driving with a validly renewed licence."
[10:52 AM] State Sol. Murphy: "Judge, while the renewal may have been in progress, at the time of the stop the defendant could not produce a valid driving licence as required under Section 38. The Garda acted within her authority based on the document presented."
[10:55 AM] Judge McCarthy: "The court has heard both sides. I will now deliver my judgment."

12.3.3. 3c. Multi-Party PQ Signing of Session Transcript

1. The complete transcript T is displayed on the courtroom signing terminals for all 5 participants to review.
2. A minor correction is proposed by Sol. Fitzpatrick (the spelling of "Síochána" is corrected); the amendment is appended.
3. Final hash: $h_T = \text{SHA-3-256}(T)$.
4. Each of the 5 participants signs using their hybrid PQ keys:

$$\sigma_i = \text{Ed25519.Sign}(sk_{i,\text{Ed}}, h_T) \parallel \text{ML-DSA-65.Sign}(sk_{i,\text{ML}}, h_T) \quad \text{(3,357 bytes each)} \tag{10}$$

5. Total signature data for session: $5 \times 3{,}357 = 16{,}785$ bytes.
6. Transcript stored on IPFS (CID_T); on-chain record submitted to Fabric; all 5 PQ signatures verified by chaincode before commit.

12.4. Step 4: Verdict

Judge McCarthy delivers the verdict in the same session.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

Verdict — Case DC-Cork-2027-Traffic-01193

Findings of Fact:

1. The defendant, Mr. Seán O'Brien, was stopped on 15 January 2027 while driving vehicle 211-C-4567 on the South Link Road, Cork.
2. The physical driving licence card presented to Garda Sergeant Brennan showed an expiry date of 31 December 2026.
3. Exhibit D-1 establishes that the defendant applied for licence renewal via the NDLS online portal on 20 December 2026—eleven days before the expiry date.
4. Exhibit D-2 establishes that the NDLS processed and approved the renewal on 3 January 2027 and dispatched the new licence card on 8 January 2027.
5. Exhibit D-3 establishes that the new licence card was delivered by An Post on 18 January 2027—three days after the Garda stop.
6. The defendant was therefore driving with a *validly renewed* licence, albeit one whose replacement card had not yet been delivered due to postal processing times.

Legal Reasoning:

Section 38 of the Road Traffic Act 1961 (as amended) requires a person driving a mechanically propelled vehicle in a public place to hold a valid driving licence. However, the NDLS online renewal system, operated under statutory authority by the Road Safety Authority, issues a digital confirmation of renewal that constitutes evidence of valid licence status during the processing period.

The court considers the judgment in *DPP v. Keane* [2018] IECA 112, in which the Court of Appeal held that where a person has taken all reasonable steps to comply with licensing requirements and a delay is attributable to an administrative process, strict criminal liability should not attach. Furthermore, under Section 5 of the Electronic Commerce Act 2000, electronic records produced by authorized government systems carry evidentiary weight equivalent to paper records.

The court finds that the defendant held a validly renewed licence at the time of the offence. The physical card's outdated expiry date does not negate the digital renewal approved by the NDLS. The Garda acted in good faith based on the physical document presented, but the digital evidence produced by the defence is dispositive.

Order:

The charge under Section 38 of the Road Traffic Act 1961 is **dismissed**. No penalty points are endorsed. No fine is imposed. No order as to costs.

Judge's Comment:

"This case highlights a gap between the NDLS digital renewal system and the physical licence card issuance process. The court recommends that the NDLS and the Road Safety Authority implement a system whereby drivers who have completed an online renewal receive an instant digital confirmation with a QR code that can be verified by An Garda Síochána during roadside stops, eliminating the need to rely on physical cards during the postal processing period. Furthermore, An Garda Síochána should be directed to check the NDLS database before issuing Fixed Charge Notices for expired licences. This would prevent unnecessary court proceedings and reduce the burden on the District Court."

12.5. Step 5: PQ Cryptographic Sealing of Verdict

1. Judge McCarthy's verdict document V is finalized in the TRUST-Court system.
2. Hash computed: $h_V = \text{SHA-3-256}(V)$ — 32 bytes.
3. **Triple hybrid archival signature:**

$$\begin{aligned}\sigma_{\text{verdict}} = {} & \text{Ed25519.Sign}(sk_{\text{McC,Ed}}, h_V) \quad \text{(64 bytes)} \\ & \| \ \text{ML-DSA-65.Sign}(sk_{\text{McC,ML}}, h_V) \quad \text{(3,293 bytes)} \\ & \| \ \text{SLH-DSA.Sign}(sk_{\text{McC,SLH}}, h_V) \quad \text{(35,664 bytes)}\end{aligned} \tag{11}$$

   Total signature: 39,021 bytes (≈38 KB).
4. Verdict stored on IPFS: $\text{CID}_V =$ `bafybei...`.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

5. Committed to Fabric (Courts Service of Ireland channel).
6. SHA-3-256 hash anchored to Polygon PoS: transaction hash `0x7f9a...`
7. Published on `transparency.courts.ie` in English and Irish.

12.6. Step 6: Public Verification

Any citizen can now verify this verdict:

1. Visit `transparency.courts.ie/verify`.
2. Enter case number `DC-Cork-2027-Traffic-01193` or scan the QR code on the verdict document.
3. The portal retrieves the verdict from IPFS, recomputes SHA-3-256, and compares with the on-chain Polygon anchor.
4. The portal verifies all three components of Judge McCarthy's triple PQ signature against his published X.509v3 certificate.
5. A green checkmark confirms: "Verdict integrity verified. All post-quantum signatures valid."

But how does the public know this case exists? Mr. O'Brien knows his own case number, but what about a different driver in Galway facing the same problem next month? She does not need to know this specific case number. She can search the Precedent Search API for "expired licence NDLS online renewal charge dismissed Road Traffic Act" and discover this verdict instantly (Channel 2). Alternatively, she may see it on the public verdict feed filtered by "District Court Cork + traffic" (Channel 1), read about it in a news article on `rte.ie` or `thejournal.ie` with an embedded verification link (Channel 6), or learn about it from a Citizens Information Centre or FLAC (Free Legal Advice Centres) clinic (Channel 7). The QR code printed on the court order (Channel 4) can also be shared. A complete description of all seven discovery channels is provided in Section 14.

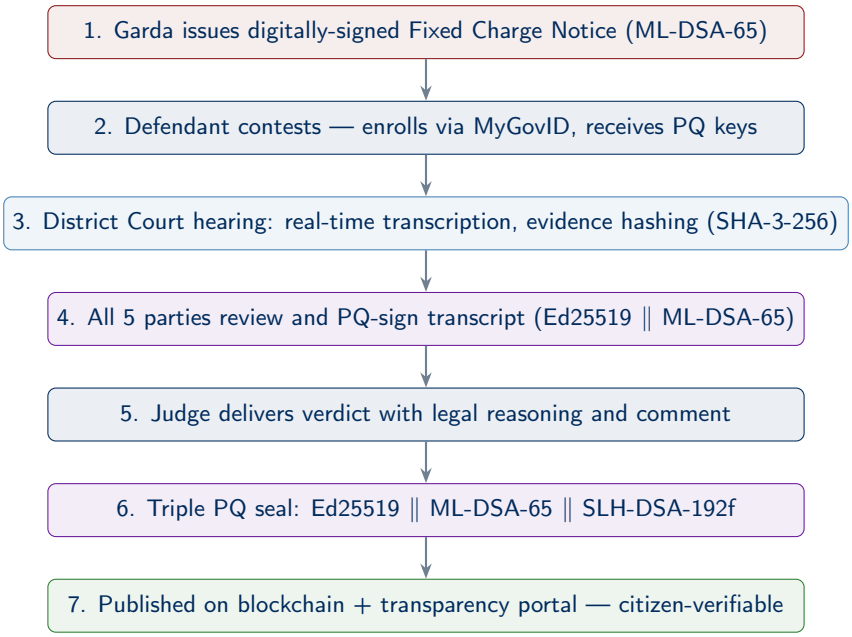

Figure 6. Complete lifecycle of the Irish traffic offence case through TRUST-Court: from Garda Fixed Charge Notice to citizen-verifiable, post-quantum sealed public verdict.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

13. Comparative Analysis: USA, India, and Ireland

Table 2. Deployment Comparison: United States, India, and Ireland

Dimension	United States	India	Ireland
Court Structure	94 districts, 13 circuits, SCOTUS + 50 states	SC + 25 HCs + 700 DCs + Taluk	Supreme, Court of Appeal, High, Circuit, District
Annual Caseload	∼80M/year	∼50M backlog + 30M new/year	∼600K/year
Identity System	Login.gov (IAL2)	Aadhaar (1.3B enrolled)	MyGovID + Public Services Card
Legal Framework	E-SIGN Act, UETA	IT Act 2000 (Sec. 3A)	eIDAS (EU), Electronic Commerce Act 2000
PQ Mandate	NSM-10, CNSA 2.0	No explicit mandate yet	EU Cyber Resilience Act, eIDAS 2.0
Languages	English	22 scheduled languages	English & Irish
Estimated Cost	$2.5–4B (5 yr)	$1.8–3B (7 yr)	€50–100M (3 yr)
Key Challenge	State-federal coordination	Scale, connectivity, literacy	Legacy system modernization

14. Precedent Discovery and Open Legal Transparency

One of the most powerful yet underexplored benefits of TRUST-Court is its potential to transform how legal precedents are discovered, cited, and verified. In most judicial systems today, finding relevant past judgments is difficult, expensive, and often incomplete. Lawyers must search through fragmented databases, pay for access to proprietary legal repositories, and rely on manual citation chains that may miss important rulings. Ordinary citizens—who have every right to understand the law that governs them—are often entirely shut out of this process. TRUST-Court changes this fundamentally by making every published verdict, its underlying problem statement, and its legal reasoning **openly searchable, freely accessible, and cryptographically verifiable** by anyone.

14.1. The Problem: Opaque Judicial Records

To understand why this matters, consider the current state of affairs in the two jurisdictions studied in this paper:

In the United States, the PACER system charges $0.10 per page to access federal court documents. While this fee seems small, it generates over $150 million per year and creates a meaningful barrier for independent researchers, small law firms, public interest organizations, and individual citizens. Many state court records are even less accessible, scattered across county-level websites with inconsistent formats and no search capability. A lawyer preparing a defense in a routine traffic case cannot easily discover that a judge in a neighboring district ruled favorably on an identical issue six months ago.

In India, the situation is more acute. While the eCourts portal provides basic case status information, the full text of most lower court judgments is not published online at all. High Court and Supreme Court judgments are available on individual court websites, but there is no unified, searchable database covering all courts. A defense advocate in a district court in Pune has no practical way to discover that a magistrate in Chennai ruled on an identical legal question the previous month. This information asymmetry disadvantages litigants, creates inconsistent outcomes, and undermines the principle that like cases should be decided alike.

14.2. TRUST-Court's Precedent Transparency Architecture

TRUST-Court addresses this problem through a dedicated **Precedent Discovery Layer** integrated into the Layer 5 Public Transparency Portal. Every published verdict is not merely stored—it is

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

structured, indexed, and made searchable so that any person, whether a Supreme Court advocate or an ordinary citizen, can discover relevant past rulings.

14.2.1. Structured Verdict Metadata

When a judge issues a verdict through TRUST-Court, the system automatically extracts and indexes the following structured metadata alongside the full verdict text:

1. **Problem Statement (Case Summary):** A concise description of the legal dispute—what happened, who is involved, and what legal question the court was asked to decide. For example: "Whether a driving licence renewed online through the NDLS but not yet reflected in the physical card constitutes a valid licence under Section 38 of the Road Traffic Act 1961 (Ireland)."
2. **Legal Provisions Invoked:** All statutes, sections, and regulations cited by the parties and the court (e.g., "Road Traffic Act 1961, Section 38 (Ireland)"; "IT Act 2000, Section 66C (India)"; "35 U.S.C. §284 (USA)").
3. **Precedents Cited:** All prior judgments cited in the ruling, linked to their own TRUST-Court records where available (e.g., "*State of Kerala v. Unni* (2019)"; "*Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005)").
4. **Legal Reasoning Tags:** Machine-readable tags categorizing the legal reasoning applied (e.g., "doctrine of equivalents," "digital evidence admissibility," "online renewal validity").
5. **Outcome Classification:** Whether the case resulted in acquittal, conviction, damages awarded, injunction granted, fine set aside, etc., with the specific order.
6. **Court and Jurisdiction:** The court level, geographic jurisdiction, and presiding judge.
7. **Cryptographic Verification Link:** The Polygon anchor hash and IPFS CID, enabling anyone to verify the verdict's authenticity directly from the search results.

All of this metadata is itself included in the SHA-3-256 hash that is PQ-signed by the judge, ensuring that the metadata cannot be altered or misrepresented after publication.

14.2.2. Open Precedent Search API

TRUST-Court exposes a **public, free-of-charge Precedent Search API** that enables any person or software application to search the entire corpus of published verdicts. The API supports the following query types:

Table 3. Precedent Search API — Query Types and Use Cases

Query Type	Example Query	Use Case
Statute Search	"Section 38 RTA 1961"	Find all cases involving a specific legal provision
Keyword Search	"online license renewal"	Discover cases with similar factual scenarios
Outcome Search	"Section 66C + acquittal"	Find cases where a specific charge led to acquittal
Precedent Chain	"Cases citing *Kerala v. Unni*"	Trace how a precedent has been applied across courts
Jurisdiction Filter	"District Court Cork + traffic"	Find comparable rulings within a specific court
Judge's Reasoning	"digital evidence + admissibility"	Research how courts have handled a legal doctrine
Similar Problem	"expired document + valid renewal"	AI-assisted discovery of analogous fact patterns

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

14.2.3. Precedent Verification and Citation

A critical feature of TRUST-Court's precedent system is that **every cited precedent can be cryptographically verified**. When a lawyer cites a past judgment in a new case, the citation includes the TRUST-Court verification hash. The court (or opposing counsel, or any member of the public) can instantly verify that the cited judgment is authentic, complete, and has not been altered or selectively quoted.

This eliminates a class of problems that currently plague judicial systems: misquoted judgments, fabricated citations, and selective excerpting that misrepresents a court's reasoning. In TRUST-Court, a citation is not just a reference to a document—it is a **cryptographic commitment** to the exact content of the referenced verdict.

The citation format is:

$$\text{Citation} = \{\text{CaseID}, \text{CourtID}, \text{Date}, h_V, \text{CID}_V, \text{PolygonTxHash}\} \tag{12}$$

where $h_V = \text{SHA-3-256}(V)$ is the verdict hash, CID_V is the IPFS content identifier, and the Polygon transaction hash provides a public, immutable anchor. Any recipient of this citation can independently verify the full verdict in seconds.

14.3. How This Changes Legal Practice

14.3.1. For Lawyers

Consider Ms. Ciara Fitzpatrick, the defence solicitor from Case Study 3 (Section 12). Before arguing that an online-renewed licence is valid despite the physical card not yet being delivered, she needs to find precedents supporting her position. In the current system, she would need to search multiple legal databases (BAILII, the Courts Service website, and commercial services such as Justis or Westlaw IE), each with different coverage, different search interfaces, and subscription fees.

With TRUST-Court's Precedent Search API, Ms. Fitzpatrick can issue a single query—"online renewal valid expired licence Road Traffic Act"—and instantly receive a list of all published verdicts across every TRUST-Court-connected court in Ireland (and indeed across jurisdictions) that have addressed this issue. Each result includes the problem statement, the court's reasoning, the outcome, and a cryptographic verification link. She can cite these precedents in her argument with the confidence that the court can verify them instantly.

14.3.2. For Judges

Judges benefit equally. When Judge McCarthy hears the traffic case, he can search the precedent database to see how other District Court judges have ruled on identical facts. This promotes **judicial consistency**—the principle that similar cases should produce similar outcomes regardless of which court hears them. Currently, a judge in Cork may be completely unaware that a judge in Dublin ruled on the same legal question last month. TRUST-Court eliminates this information gap.

14.3.3. For Citizens

Perhaps most importantly, TRUST-Court's open precedent system empowers **ordinary citizens**. A person facing a traffic fine, a tenant disputing an eviction, or a small business owner challenging a regulatory penalty can search the precedent database to understand how courts have ruled on similar issues. This does not replace the need for legal counsel, but it dramatically reduces the information asymmetry between citizens and the legal system.

For example, Mr. Seán O'Brien, before even engaging a solicitor, could search "expired licence NDLS online renewal charge dismissed" and discover that multiple courts have ruled in favour of defendants in similar situations. Armed with this knowledge, he can make an informed decision about whether to contest the charge and can provide his solicitor with relevant precedents from the outset.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

14.3.4. For Legal Researchers and Journalists

Law students, academic researchers, policy analysts, and investigative journalists gain access to the complete corpus of published judicial decisions with full-text search, structured metadata, and cryptographic authenticity guarantees. This enables large-scale empirical legal research that is currently impossible in most jurisdictions—for example, analyzing sentencing patterns across different courts, tracking the adoption of new legal doctrines, or identifying systematic inconsistencies in judicial outcomes.

14.4. Precedent Discovery Flow

Figure 7 illustrates the complete precedent discovery and citation verification workflow.

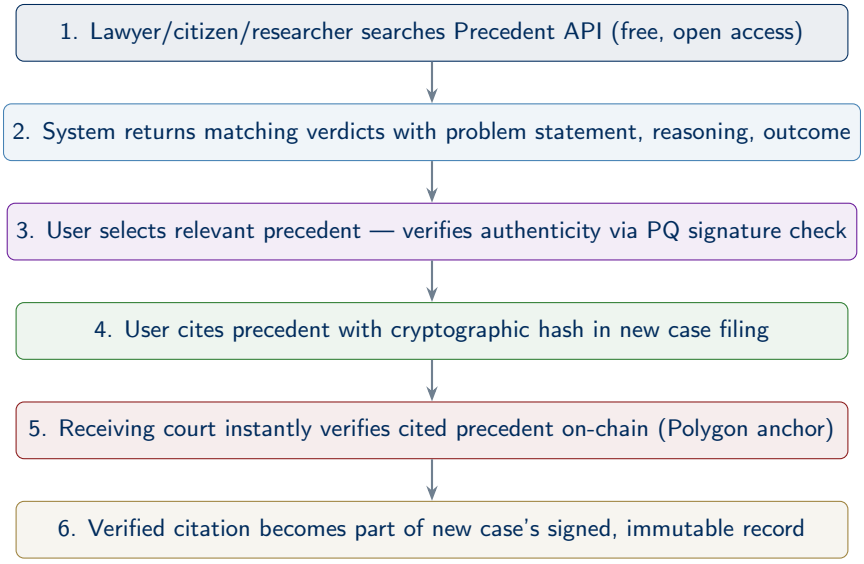

Figure 7. Precedent discovery and cryptographically verified citation workflow. Every cited precedent can be independently verified by any party.

14.5. How Does the General Public Discover Cases?

A natural question arises: if public verification requires a case number or QR code, **how does a member of the general public—someone who is not a party to the case—come to know that a particular verdict exists and learn its case number?** In today's systems this is a genuine barrier; in TRUST-Court, it is addressed through seven complementary discovery channels, ensuring that no one needs to already know a case number to find relevant judicial decisions.

14.5.1. Channel 1: Proactive Public Notification Feed

TRUST-Court's transparency portal maintains a **real-time public verdict feed**—similar to a news feed or government gazette—where every newly published, non-sealed verdict appears automatically upon publication. This feed is:

- Accessible at `transparency.ecourts.gov.in/feed` (India) or `transparency.uscourts.gov/feed` (USA).
- Filterable by court, jurisdiction, date range, case type (civil, criminal, traffic, family, etc.), and legal topic.
- Available as an RSS/Atom feed, a JSON API, and a human-readable web page, so that news organizations, legal blogs, research institutions, and individual citizens can subscribe.

A journalist covering cybercrime in Mumbai, for example, can subscribe to the feed filtered by "Sessions Court Mumbai + IT Act" and automatically receive notification whenever a new cybercrime verdict is published—complete with the case number, problem summary, outcome, and verification link.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

14.5.2. Channel 2: Full-Text and Topic Search (No Case Number Required)

The Precedent Search API described in Section 14 does **not require a case number**. Any person can search by:

- **Keywords:** "phishing bank identity theft Mumbai" returns all published verdicts matching those terms.
- **Legal provision:** "Section 66C IT Act" returns every case decided under that statute.
- **Outcome type:** "dismissed + Section 38 Road Traffic Act" finds all cases where a driving charge was dismissed.
- **Natural language:** "Can I be fined if I renewed my driving license online but the physical card wasn't updated?" (the system uses semantic search to find verdicts with matching fact patterns).

This means that a citizen who has never heard of case `DC-Cork-2027-Traffic-01193` can still discover it by searching for the legal issue they care about. Every search result includes the case number, a one-paragraph problem summary, the outcome, and a one-click verification link.

14.5.3. Channel 3: Automatic Party and Stakeholder Notifications

When a verdict is published, TRUST-Court automatically notifies all **directly interested parties** via the contact information in their enrollment profiles:

- **Parties to the case** (plaintiff, defendant, accused) receive SMS, email, and in-app notification with the case number, outcome summary, QR code, and verification link.
- **Enrolled lawyers** in the case receive the same notification plus a link to the full signed verdict on IPFS.
- **Victims** (in criminal cases with identified victims, as in Case Study 2) receive notification that a verdict has been issued and can verify it.
- **Concerned government agencies** (e.g., the Regional Transport Office in a traffic case, the bank's fraud department in a cybercrime case) receive structured notifications via the Open Data API.

14.5.4. Channel 4: QR Codes on Physical Documents

Every verdict document—whether displayed on screen, printed, or communicated to parties—includes a prominently placed **QR code** that encodes the verification URL. This QR code can be:

- Printed on official court orders served to parties.
- Displayed on courtroom screens when the verdict is announced.
- Included in SMS/email notifications to parties.
- Published alongside the verdict on government websites.
- Printed in newspapers or shown in news broadcasts when media outlets report on cases.

Anyone who sees the QR code—whether on a physical court order, a newspaper article, or a television broadcast—can scan it with any smartphone to instantly verify the verdict's authenticity. No prior knowledge of the case number is required.

14.5.5. Channel 5: Court Daily Cause Lists and Gazette Publication

Courts already publish daily **cause lists** (the schedule of cases to be heard on a given day) and periodic **gazettes** (official publications of court orders). In TRUST-Court, these are enhanced:

- Daily cause lists include hyperlinks to the TRUST-Court records for each listed case.
- When a verdict is delivered, the cause list entry is updated with the outcome and verification link.
- Official gazettes (the *Gazette of India* or the *Federal Register*) include TRUST-Court verification hashes for all published judicial orders.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

14.5.6. Channel 6: News Media and Public Interest Integration

TRUST-Court provides a dedicated **Media API** endpoint that news organizations can integrate into their reporting workflows. When a journalist writes about a court case, they can embed the TRUST-Court verification widget directly in their article. Readers of the news article can click the widget to verify the cited verdict themselves, rather than relying solely on the journalist's account. This creates a new standard of accountability in legal journalism: every claimed court ruling can be independently checked by the reader.

14.5.7. Channel 7: Legal Aid Clinics and Community Outreach

For citizens who lack internet access or digital literacy, TRUST-Court supports integration with **legal aid clinics, Common Service Centres (CSCs)** in India, and public library terminals. Legal aid workers can search the precedent database on behalf of citizens, print verification-linked summaries, and explain how the verification process works. In India, the network of over 400,000 CSCs can serve as access points, ensuring that even rural citizens without smartphones can discover and verify court decisions relevant to their situation.

No One Needs to Know a Case Number in Advance

The seven discovery channels ensure that **no prior knowledge of a case number is required** to find and verify judicial decisions. Citizens discover relevant verdicts through public feeds, keyword searches, news media, community outreach, or QR codes. The case number is a convenient identifier, not a prerequisite. TRUST-Court's design ensures that the path from "I have a legal question" to "Here is a verified court ruling on that exact issue" requires nothing more than an internet connection and a search query.

14.6. Privacy-Preserving Transparency

An important consideration is that not all case details should be publicly searchable. TRUST-Court implements a nuanced privacy framework:

- **Fully public:** Verdict text, legal reasoning, outcome, statutes cited, and precedents cited. These are always searchable.
- **Redacted public:** Cases involving minors, sexual offenses, national security, or other sensitive matters are published with personal identifiers redacted. The legal reasoning and outcome remain searchable, but identifying details are removed. The PQ signature covers the redacted version (using redactable signatures where available—see Section 20, Direction 5).
- **Sealed:** Certain records (e.g., ongoing investigations, sealed juvenile records) are not published to the precedent database at all. They remain on the permissioned Fabric chain and are accessible only to authorized parties.

This graduated approach ensures that precedent transparency does not come at the cost of legitimate privacy interests, while maximizing the volume of searchable legal knowledge.

14.7. Impact on Justice System Efficiency

Open precedent discovery is expected to have a significant positive impact on judicial efficiency:

- **Reduced re-litigation:** When parties can easily discover that courts have consistently ruled a certain way on a legal question, frivolous or hopeless cases are less likely to be filed.
- **Faster case preparation:** Lawyers spend less time searching for precedents and more time on substantive legal analysis.
- **Judicial consistency:** Judges can quickly determine how peers have ruled on similar issues, reducing inconsistent outcomes across jurisdictions.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

- **Early settlement:** When both parties can see how courts have ruled on comparable facts, out-of-court settlements become more likely, reducing the burden on the court system.
- **Legal aid empowerment:** Public defenders and legal aid organizations, which often lack the budgets for premium legal databases, gain equal access to the full precedent corpus.

Open Access to Justice

We recommend that all TRUST-Court jurisdictions adopt a policy of **zero-cost access** to the Precedent Search API and the full text of published, non-sealed verdicts. Legal knowledge should not be gated behind subscription fees. When every citizen can search "cases like mine" and find cryptographically verified judicial reasoning, the law becomes truly accessible to the people it governs.

15. Post-Quantum Security Analysis

15.1. Threat Model

We consider: (1) classical adversaries, (2) quantum adversaries with CRQCs, (3) insider threats, and (4) multi-party collusion.

15.2. Security Guarantees

ML-DSA-65 is EU-CMA secure under Module-LWE/SIS in the QROM. SLH-DSA security relies only on hash function pre-image resistance. SHA-3-256 retains 128-bit PQ security under Grover. ML-KEM-768 provides IND-CCA2 security under Module-LWE.

Theorem 1: Hybrid Signature Security

The hybrid $\Sigma_{\text{hyb}} = (\text{Ed25519} \| \text{ML-DSA-65})$ is EU-CMA secure if *either* component is secure:

$$\text{Adv}^{\text{EU-CMA}}_{\Sigma_{\text{hyb}}}(\mathcal{A}) \leq \text{Adv}^{\text{EU-CMA}}_{\text{Ed25519}}(\mathcal{B}_1) + \text{Adv}^{\text{EU-CMA}}_{\text{ML-DSA}}(\mathcal{B}_2) \tag{13}$$

Theorem 2: Triple Hybrid Archival Security

The triple hybrid Σ_{triple} is EU-CMA secure if *any one* of the three schemes is secure:

$$\text{Adv}^{\text{EU-CMA}}_{\Sigma_{\text{triple}}}(\mathcal{A}) \leq \sum_{j=1}^{3} \text{Adv}^{\text{EU-CMA}}_{\Sigma_j}(\mathcal{B}_j) \tag{14}$$

All three failure modes would need to occur simultaneously for forgery. □

15.3. PQ Threat-Defense Mapping

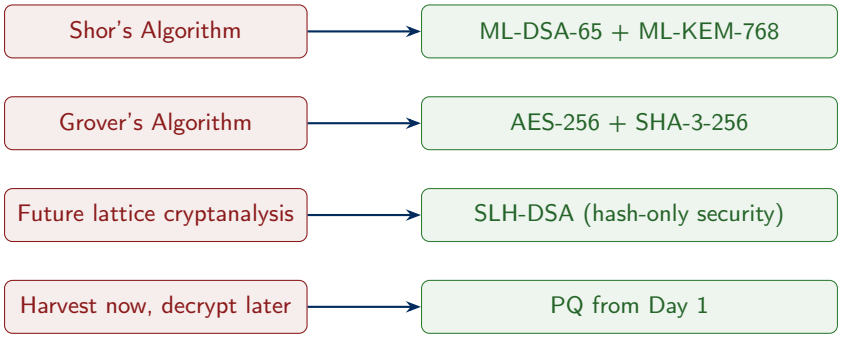

Figure 8. Post-quantum threat-defense mapping.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

16. Storage Optimization for Post-Quantum Cryptographic Data

One of the most significant practical challenges of post-quantum cryptography is the dramatically larger sizes of keys and signatures. Table 4 illustrates the scale of this problem.

Table 4. Size Comparison: Classical vs. Post-Quantum Cryptographic Objects

Object	Classical	Post-Quantum	Expansion
Signature (Ed25519 vs ML-DSA-65)	64 B	3,293 B	∼51×
Archival Sig. (SLH-DSA)	N/A	35,664 B	—
Public Key (Ed25519 vs ML-DSA-65)	32 B	1,952 B	∼61×
KEM Ciphertext	32 B	1,088 B	∼34×
Triple Hybrid Verdict Sig.	64 B	39,021 B	∼610×
5-party Session Sigs (hybrid)	320 B	16,785 B	∼52×

Scale of the problem: India processes approximately 30 million new cases per year. With an average of 5 sessions plus a verdict per case, annual signature data alone would be approximately 3.7 TB. Over a 20-year archival period, this grows to ∼74 TB—a substantial burden requiring efficient management.

16.1. Technique 1: Merkle-Tree Signature Batching

Instead of storing individual session signatures on-chain, we batch multiple sessions into a Merkle tree and store only the 32-byte root hash on-chain. Full signatures reside off-chain (IPFS) with Merkle inclusion proofs for individual verification:

$$\text{MerkleRoot} = \text{MT.Root}(\text{SHA-3-256}(\sigma_1), \ldots, \text{SHA-3-256}(\sigma_B)) \tag{15}$$

For $B = 256$ sessions, on-chain storage drops from 4.3 MB to 32 bytes—a **99.8% reduction**.

16.2. Technique 2: SLH-DSA Signature Compression

SLH-DSA signatures have internal structure (WOTS+ signatures and hypertree authentication paths) exploitable by compression. Applying zlib/DEFLATE reduces signatures from 35,664 to ∼28,000–30,000 bytes (**16–22% reduction**). Furthermore, **signature deduplication** across verdicts from the same judge within an epoch—sharing hypertree authentication paths—yields an additional **25–35% reduction**.

16.3. Technique 3: Delta Encoding for Public Key Certificates

The same participants (judges, prosecutors, frequent advocates) appear across many cases. A **certificate registry** stores each certificate once, indexed by a 16-byte CertID. Court records reference CertIDs rather than embedding full certificates. With 5 participants per record, this saves ∼10,000 bytes per record, or approximately **300 GB per year** across 30 million cases.

16.4. Technique 4: Tiered Archival Storage

Not all records are accessed equally. We implement three tiers with progressive compression:

- **Tier 1 (Hot, 0–6 months):** Full uncompressed records on SSD. Raw signatures for fast verification.
- **Tier 2 (Warm, 6 months–5 years):** LZ4 compression. SLH-DSA signatures compressed. Certificate deduplication. HDD arrays. Achieves **40–55% compression**.
- **Tier 3 (Cold, 5+ years):** Zstandard at high compression. Epoch archives. Tape/cloud cold storage. Precomputed Merkle proofs. Achieves **65–80% compression**.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

16.5. Technique 5: On-Chain Storage Minimization

The blockchain stores only the minimum for verification. Per record on-chain: Case ID (32 B), hash (32 B), IPFS CID (36 B), Merkle batch root (32 B), metadata (64 B)—total ≈**196 bytes**. All bulk data (transcripts, signatures, certificates, evidence) resides off-chain. This achieves a **99.6% reduction** versus storing full signatures on-chain.

16.6. Combined Storage Impact

Table 5. Combined Storage Optimization Impact (India, 30M cases/year)

Technique	Before	After	Reduction
On-chain (per record)	∼55 KB	196 bytes	99.6%
Cert storage (annual)	∼600 GB	∼300 GB	50%
SLH-DSA sigs (annual)	∼1.07 TB	∼0.75 TB	30%
Tiered archival (20yr)	∼74 TB	∼22 TB	70%
System-wide (20yr)	**∼74 TB**	**∼15–22 TB**	**70–80%**

These optimizations make TRUST-Court's post-quantum storage requirements comparable to a classical system, removing storage as a practical barrier to adoption.

17. Performance Analysis

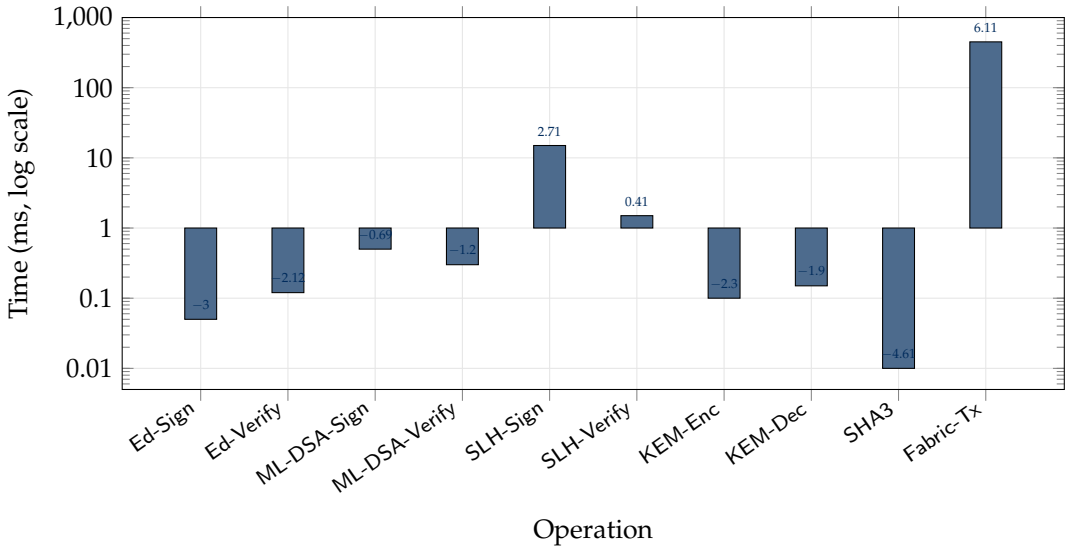

Figure 9. Latency of all cryptographic and blockchain operations (log scale). SLH-DSA signing at 15 ms is the slowest PQ operation—still fast for verdict signing.

Total end-to-end session signing: <10 seconds (excluding human review). Verdict with SLH-DSA: <11 seconds. PQ overhead is negligible.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

18. Phased Transition Roadmap

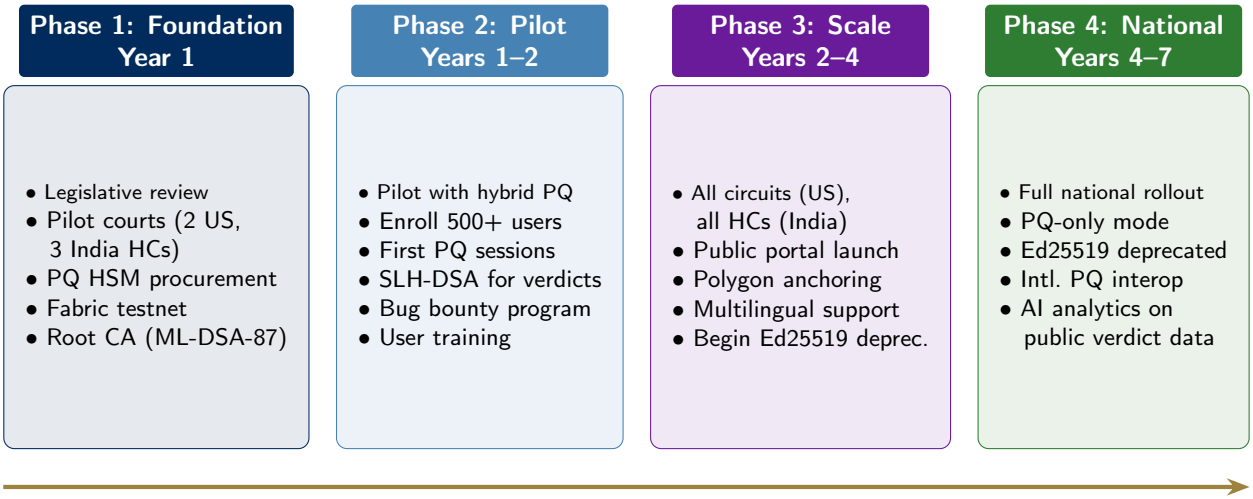

Figure 10. Four-phase transition roadmap with progressive PQ migration.

19. Complete Technology Stack

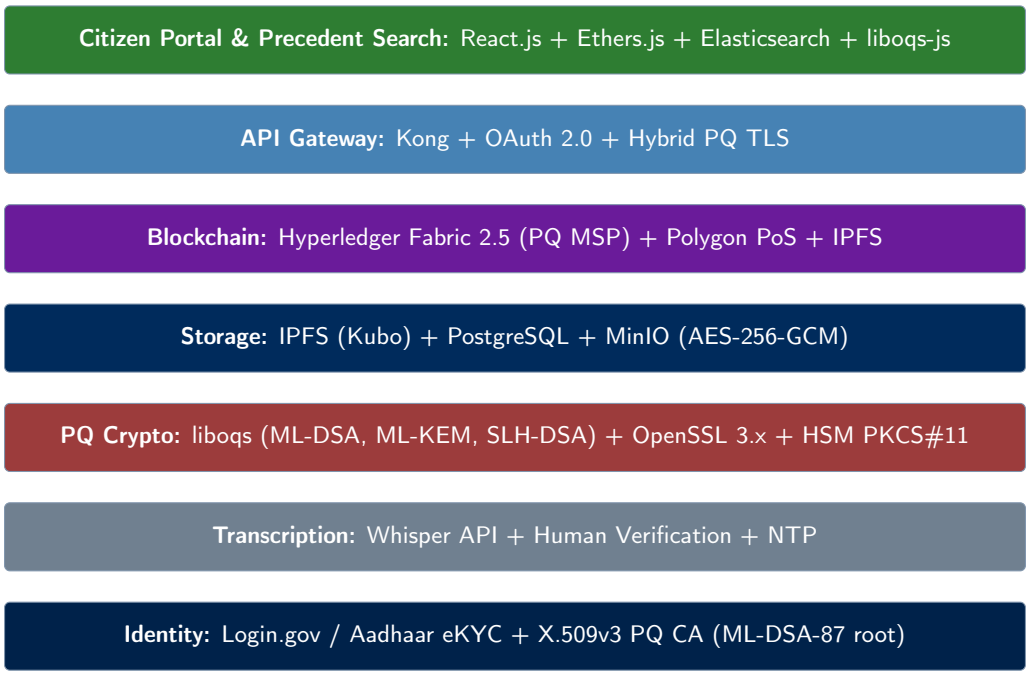

Figure 11. Complete technology stack with PQ cryptography at every layer.

Call to Action

We recommend that the **Executive Office of the President (USA)** and the **Ministry of Law and Justice (India)** convene technical working groups to evaluate this framework, targeting Phase 1 pilot deployments within 18 months. Every day of delay widens the "harvest now, decrypt later" vulnerability window for judicial records.

20. Formal Cryptographic Research Roadmap for Constitution-Grade Digital Judiciary Systems

This section serves a dual purpose: it establishes a formal security model for the TRUST-Court protocol suite, and it identifies **eleven open research problems** representing attractive directions for

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

the cryptographic community. Each problem includes a formal definition, a security game, a target theorem, and a discussion of **why this problem matters for judiciary applications** and **what makes it an attractive research direction**.

The judiciary domain presents unique constraints: extremely long archival periods (50–100+ years), public verifiability alongside selective privacy, non-technical users, and "constitution-grade" security requirements where cryptographic failure could undermine an entire branch of government.

20.1. System Model and Adversarial Setting

Let λ denote the security parameter. Let $\Pi = (\Pi_{\mathrm{ID}}, \Pi_{\mathrm{TR}}, \Pi_{\mathrm{EV}}, \Pi_{\mathrm{LOG}}, \Pi_{\mathrm{AR}})$ be a judiciary protocol suite consisting of: Π_{ID} (identity and credential lifecycle), Π_{TR} (transcript authentication), Π_{EV} (confidential evidence storage), Π_{LOG} (public transparency infrastructure), and Π_{AR} (long-term archival verification).

Adversaries are PPT algorithms $\mathcal{A}$ including external adversaries, insider adversaries (compromised judges, log operators), adaptive adversaries with key compromise capability, and quantum adversaries with polynomial-time quantum computation. Security must hold with negligible probability in λ.

20.2. Direction 1: Post-Quantum Transparency Log Security

Why this matters: Transparency logs underpin public accountability in TRUST-Court. A split-view attack—where an adversary presents different log views to different observers—would collapse the system's trustworthiness. While classical Merkle-tree logs are well-studied, their security under quantum adversaries requires new analysis.

Why it is attractive: Designing logs provably secure in the QROM requires revisiting standard collision-resistance arguments when adversaries query hash functions in quantum superposition, connecting to fundamental open questions in post-quantum hash security.

Definition 1 (Append-Only Transparency)**.** *A log $\mathcal{L}$ is append-only if no PPT adversary can produce two distinct log views $\mathcal{L}_1 \neq \mathcal{L}_2$ such that both verify under public consistency proofs while diverging on any committed entry.*

Security Game: Split-View Attack

Setup: Challenger initializes empty log $\mathcal{L}$. **Adversary Access:** $\mathcal{A}$ may request log insertions and consistency proofs. **Goal:** Output $(\mathcal{L}_1, \mathcal{L}_2)$ and proofs π_1, π_2 such that $\mathcal{L}_1 \neq \mathcal{L}_2 \wedge \mathrm{Verify}(\mathcal{L}_1, \pi_1) = \mathrm{Verify}(\mathcal{L}_2, \pi_2) = 1$.

Theorem 1 (Transparency Security Objective)**.** *If H is collision-resistant against quantum adversaries, then any Merkle-based log achieves negligible split-view advantage.*

Open problem: Construct a transparency log with a tight security reduction in the QROM.

20.3. Direction 2: Post-Quantum Key Transparency and Identity Continuity

Why this matters: Participants' keys must be rotated and may be revoked. Key transparency ensures all observers agree on current and historical keys. Without this, an adversary could register a fraudulent key for a judge and sign fake verdicts.

Why it is attractive: The migration from classical to PQ keys must itself be quantum-secure, creating windows of vulnerability that require novel composable security models. This connects to verifiable data structures, consensus, and identity management.

Definition 2 (Non-Equivocating Identity Mapping)**.** *A key transparency system guarantees that for any identity* id*, all observers see a unique, globally consistent public key history.*

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

Open problem: Design a key transparency scheme where classical-to-PQ key rotation is provably secure under a composable security model with no vulnerability window.

20.4. Direction 3: Threshold Post-Quantum Signatures

Why this matters: High-stakes operations (constitutional court rulings, apex court orders) may require multiple judges to jointly sign. Threshold signatures prevent any single compromised judge from issuing fraudulent orders.

Why it is attractive: Threshold ML-DSA is one of the most active and challenging open problems in post-quantum cryptography. Unlike classical ECDSA, lattice algebraic structure makes threshold signing significantly harder. NIST and IACR conferences have highlighted this as a priority.

Let TSig be a (t, n)-threshold signature scheme.

Definition 3 (Threshold Unforgeability)**.** *No adversary controlling fewer than t signing shares can produce a valid signature.*

Open problem: Construct an efficient (t, n)-threshold ML-DSA with $O(1)$ rounds and signature size independent of n, proven secure in the QROM.

20.5. Direction 4: Forward-Secure Post-Quantum Signatures

Why this matters: Compromise of a current signing key should not allow forging signatures on past documents. This is critical for judiciary archives spanning decades.

Why it is attractive: Forward-secure signatures from lattices are largely unexplored. Key evolution must be efficient and compose with hybrid signatures, connecting to fundamental questions about key management and tree-based constructions.

Definition 4 (Forward Security)**.** *Compromise of secret key at epoch i does not enable forgery for epochs $< i$.*

Open problem: Design a forward-secure ML-DSA variant with $O(1)$ key update time and at most logarithmic key material growth.

20.6. Direction 5: Post-Quantum Redactable Signatures

Why this matters: Courts often publish verdicts while redacting sensitive information (minors' identities, classified evidence). Redactable signatures allow authorized field removal *without invalidating the signature* on remaining content—providing mathematical guarantees beyond simple text blacking.

Why it is attractive: Redactable signatures from lattice or hash assumptions are almost completely unexplored, connecting to commitment schemes, chameleon hashes, and sanitizable signatures.

Definition 5 (Sanitizable Authenticity)**.** *A redactable signature permits authorized removal of fields without enabling insertion or modification of non-redacted content.*

Open problem: Construct a post-quantum redactable signature based on Module-LWE or hash functions with formal proof of non-expansion.

20.7. Direction 6: Post-Quantum Attribute-Based Encryption

Why this matters: Court evidence has complex access control—a medical report accessible to the judge and attorneys but not the public; sealed juvenile records accessible only to the presiding judge. ABE enables cryptographic, fine-grained access control.

Why it is attractive: Post-quantum ABE is emerging with limited expressiveness and efficiency. Judiciary provides concrete, well-defined access policies driving practical scheme design.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

Definition 6 (Policy Confidentiality)**.** *Ciphertext encrypted under access policy $\mathcal{P}$ reveals no information about plaintext to unauthorized parties.*

Open problem: Construct practical lattice-based ABE supporting conjunctive policies over judicial roles, with ciphertext size sublinear in the number of attributes.

20.8. Direction 7: Post-Quantum Searchable Encryption

Why this matters: Authorized users need to search encrypted databases of millions of records (judges researching precedents, prosecutors finding related cases) without decrypting everything.

Why it is attractive: Post-quantum SSE with forward privacy (new documents don't leak past query information) and backward privacy (deleted documents don't leak future query information) is rare. Judiciary demands unusually strong guarantees since search patterns could reveal investigative information.

Definition 7 (Forward Privacy)**.** *Search queries do not reveal information about past document insertions.*

Open problem: Design post-quantum SSE with forward and backward privacy supporting conjunctive keyword queries with sublinear search time.

20.9. Direction 8: Post-Quantum Zero-Knowledge Public Verification

Why this matters: ZK proofs enable proving a verdict was properly signed without revealing the judge's identity (witness protection), or that evidence satisfies criteria without revealing the evidence itself.

Why it is attractive: Post-quantum ZK systems (SNARKs, STARKs) are frontier research. Judiciary motivates specific optimizations: proofs small enough for QR codes, verification on consumer devices. This connects to lattice-based SNARKs, hash-based proof systems, and recursive composition.

Definition 8 (Succinct Verifiability)**.** *A verifier checks validity of judicial claim using proof π of size polylogarithmic in transcript size.*

Open problem: Construct a post-quantum SNARK with proof sizes under 1 KB suitable for judicial verdict verification, with verification time under 50 ms on a smartphone.

20.10. Direction 9: Post-Quantum Accumulators and Vector Commitments

Why this matters: The court system must efficiently prove that a case record *is* (or *is not*) part of the official judicial record set. Accumulators and vector commitments enable compact membership proofs for large sets.

Why it is attractive: Lattice-based accumulators with efficient batch updates and compact membership witnesses are an open problem, with applications extending far beyond judiciary systems.

Definition 9 (Dynamic Membership)**.** *Given commitment C to set S, prover can show $x \in S$ with witness w.*

Open problem: Construct a dynamic post-quantum accumulator with $O(\log n)$ witness size and $O(1)$ update time, secure under standard lattice assumptions.

20.11. Direction 10: Adversarial Timestamping

Why this matters: If a record is anchored at time t, no adversary should be able to claim it was anchored earlier. This prevents backdating of court documents.

Why it is attractive: Combining post-quantum hash functions with distributed timestamping protocols creates novel security models where anchor-chain integrity must be analyzed under quantum adversaries.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

Definition 10 (Temporal Immutability). *If record r is anchored at time t, no adversary can produce valid anchor at earlier time $t' < t$.*

Open problem: Prove that linked-timestamping with SHA-3 achieves temporal immutability against quantum adversaries under standard assumptions.

20.12. Direction 11: Post-Quantum Verifiable Delay Functions

Why this matters: VDFs ensure that certain operations take a minimum amount of real time, preventing adversaries from rushing processes (e.g., ensuring minimum deliberation periods before verdict sealing). They can also provide fair randomness for judge assignment.

Why it is attractive: Existing VDF constructions rely on classical assumptions (groups of unknown order, isogenies). Post-quantum VDFs from lattice or hash assumptions are essentially an open field, with high impact across blockchain, cryptography, and distributed systems.

Definition 11 (Sequential Hardness). *Computing $f(x)$ requires T sequential steps, while verification requires* $\mathrm{polylog}(T)$.

Open problem: Construct a VDF from post-quantum assumptions with efficient verification and provable sequential hardness against quantum parallel adversaries.

20.13. Unified Composability Objective

Definition 12 (Constitution-Grade Security). *Protocol suite Π achieves constitution-grade security if:*

1. *All subprotocols satisfy their respective security games.*
2. *Security composes under concurrent execution.*
3. *Security holds against adaptive quantum adversaries.*
4. *Long-term archival verification remains valid for $T \gg 20$ years.*

Grand Challenge

Construct a post-quantum judiciary stack satisfying:

$$\mathrm{Adv}_{\Pi}^{\mathcal{A}}(\lambda) \leq \mathrm{negl}(\lambda)$$

for all adversary classes defined above, under realistic deployment assumptions and institutional insider models.

20.14. Research Deliverables (Formal Targets)

The following represent concrete, publishable research targets for the community:

- Formal security proofs for threshold ML-DSA variants with practical round complexity.
- Composable hybrid-to-PQ migration framework with reduction proofs and zero-downtime guarantees.
- Leakage-bounded searchable encryption tailored to judiciary threat models with quantified leakage profiles.
- Post-quantum ZK verification circuits for transcript validity optimized for on-chain verification.
- Long-term cryptographic agility model with provable safety margins across algorithm generations.
- Storage-efficient PQ signature aggregation schemes with formal security under batch verification.
- Practical post-quantum redactable signatures supporting hierarchical redaction policies.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

21. Conclusions

Courts exist to protect truth, yet judicial records in many systems remain vulnerable to delay, dispute, or manipulation. This paper introduced **TRUST-Court** (*Tamper-Resistant Records for Universal Secure Transparency*), a practical framework for a digital judiciary in which every hearing, document, and verdict becomes a *verifiable fact*. By combining post-quantum cryptography, real-time transcript authentication, and blockchain-based anchoring, TRUST-Court ensures that once a judicial record is created, it cannot be altered without detection.

In the proposed system, court proceedings are captured in real time and digitally signed by all participants, creating a mathematically verifiable record of what occurred in the courtroom. Final verdicts are sealed using multiple layers of modern cryptographic protection and anchored to a distributed ledger, allowing any citizen to independently confirm the authenticity and integrity of judicial documents. The framework is designed to remain secure even in a future where quantum computers threaten today's classical cryptographic systems.

Beyond technological modernization, TRUST-Court strengthens transparency and public confidence. Citizens can verify judgments, lawyers can discover reliable precedents, and researchers can analyze judicial outcomes with cryptographic assurance that records are genuine. By transforming court archives into openly searchable and verifiable legal knowledge, TRUST-Court moves judicial systems from opaque record keeping toward accountable and transparent justice.

With phased deployment and careful integration into existing legal infrastructures, TRUST-Court offers a realistic path for governments to safeguard judicial integrity for decades to come. In the digital era, trust in justice should not rely solely on institutions—it should be reinforced by mathematics.

Disclaimer on Names and Case Scenarios

The names of individuals, organizations, and case scenarios used in this paper are purely illustrative and are included solely for explanatory and educational purposes. Any resemblance to real persons, institutions, companies, or legal cases is entirely coincidental.

The case studies presented (including examples from the United States, India, and Ireland) are hypothetical demonstrations designed to illustrate how the proposed TRUST-Court framework could operate in practical judicial environments. They do not represent actual legal proceedings, real litigants, or real court decisions.

These fictional scenarios are intended only to clarify the technical workflow, cryptographic processes, and system architecture described in this work.

References

1. NIST, "FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA)," Aug. 2024.
2. NIST, "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)," Aug. 2024.
3. NIST, "FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA)," Aug. 2024.
4. NIST, "FIPS 202: SHA-3 Standard," Aug. 2015.
23. D.J. Bernstein et al., "EdDSA: High-speed signatures," *J. Crypt. Eng.*, 2(2):77–89, 2012.
6. P.W. Shor, "Algorithms for quantum computation," *Proc. 35th FOCS*, 1994.
7. L.K. Grover, "A fast quantum algorithm for database search," *Proc. 28th STOC*, 1996.
8. Hyperledger Foundation, "Fabric v2.5 Documentation," 2024.
9. Polygon Labs, "Polygon PoS Documentation," 2024.
10. NIST, "SP 800-63-4: Digital Identity Guidelines," Dec. 2024.
11. Govt. of India, "eCourts Mission Mode Project Phase III," 2023.
12. Admin. Office of the US Courts, "PACER," 2024.
13. UIDAI, "Aadhaar Authentication API v2.5," 2024.
14. European Parliament, "eIDAS Regulation (EU) 910/2014," 2014.
15. US Congress, "E-SIGN Act," 2000.
16. J. Benet, "IPFS — Content Addressed P2P File System," arXiv:1407.3561, 2014.
17. IETF, "draft-ounsworth-pq-composite-sigs," 2024.
18. The White House, "NSM-10: Quantum Computing and Cryptographic Systems," May 2022.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 March 2026 doi:10.20944/preprints202603.0442.v1

19. NSA, "CNSA 2.0 Advisory," Sep. 2022.
20. Open Quantum Safe Project, "liboqs," 2024. https://openquantumsafe.org/
21. L. Ducas et al., "CRYSTALS-Dilithium," *TCHES*, 2018.
22. R. Avanzi et al., "CRYSTALS-Kyber," *Euro S&P*, 2019.
23. D.J. Bernstein et al., "SPHINCS+," NIST PQ submission, 2022.
24. Road Traffic Act 1961, Government of Ireland (as amended by Road Traffic Act 2006), Section 38.
25. Electronic Commerce Act 2000, Government of Ireland, Section 5.
26. Supreme Court of India, "Report of the e-Committee on Digitization," 2023.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

© 2026 by the author(s). Distributed under a Creative Commons CC BY license.