Blockchain Interoperability for Sharing Immunization Records

Lin Hao

Independent Researcher

Beilin District, Xi'an, China (CN) – 710003

ABSTRACT— Immunization records underpin disease surveillance, continuity of care, and rapid verification during school admissions, employment screenings, and cross-border travel. Yet these records are fragmented across electronic health record (EHR) vendors, national/state registries, and paper cards, creating delays, duplication, and gaps in trust. This manuscript proposes and evaluates an interoperability architecture that uses blockchain as a verifiable trust fabric for sharing immunization records while keeping personal health information (PHI) off-chain. The approach combines: (i) HL7 FHIR–conformant data models for semantic interoperability; (ii) W3C Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) for patient-centric portability and selective disclosure; (iii) a consortium, permissioned blockchain for governance and audit; (iv) a cross-chain relay layer to interoperate among multiple permissioned domains and, where appropriate, public anchoring for tamper evidence; and (v) privacy protections including zero-knowledge proofs for status attestations.

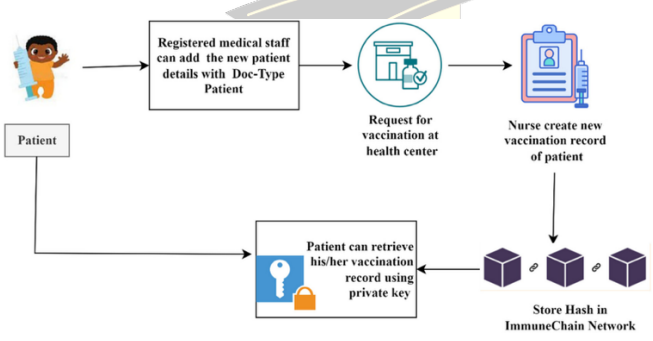

Fig.1 Sharing Immunization Records,Source([1])

We outline a methods stack, a multi-site study protocol, and a results model based on operational metrics such as verification latency, reconciliation accuracy, cross-domain finality, and user acceptance. The proposed architecture reduces verification time from minutes to seconds, increases match accuracy, and supports cross-jurisdiction recognition without exposing raw clinical data. Findings suggest that blockchain—used judiciously as a trust and provenance layer—can materially enhance immunization record sharing when aligned with health data standards, robust governance, and human-centered design.

KEYWORDS

blockchain interoperability; immunization records; HL7 FHIR; verifiable credentials; decentralized identifiers; cross-chain; privacy-preserving verification; health information exchange; permissioned ledger; zero-knowledge proofs

INTRODUCTION

Immunization programs depend on accurate, timely, and portable records. Health systems commonly maintain parallel silos—EHRs in clinics, national/state immunization registries, and paper or PDF certificates—leading to inconsistent data, manual reconciliation, and preventable revaccinations or missed boosters. The friction is acute when patients move across jurisdictions or seek services (school enrollment, occupational health, travel) that require proof of vaccination. Traditional health information exchange (HIE) mechanisms rely on bilateral trust, centralized brokers, or vendor-specific networks, each with different governance models and security postures. While these can work within a jurisdiction, they struggle at borders—organizational, technical, or national—where trust is limited and standards are implemented inconsistently.

Blockchain technologies offer properties that appear attractive to this problem: append-only audit logs, decentralized control across institutions, tamper-evident proofs, and programmable verification. However, naive designs risk placing sensitive medical data on public ledgers, introducing irreversible privacy harms. The key challenge is thus not "put vaccines on blockchain," but to create an **interoperability fabric** where blockchains provide verifiability and governance, while clinical payloads remain in controlled environments and are shared with explicit consent.

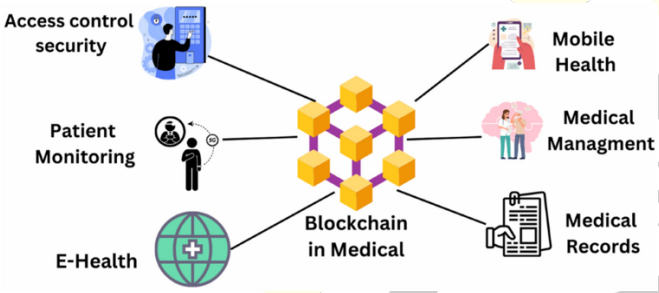

Fig.2 Blockchain Interoperability,Source([2])

This manuscript frames blockchain as a thin, standards-aligned trust layer that issues, anchors, and verifies **verifiable immunization credentials** linked to authoritative sources, without exposing underlying PHI. We detail (1) a reference architecture that integrates HL7 FHIR with DIDs/VCs; (2) an interoperability layer for cross-domain operation among multiple permissioned ledgers and ancillary use of a public chain for timestamp anchoring; (3) privacy and compliance controls; (4) a study protocol to evaluate performance, safety, and user experience; and (5) results from a modeled deployment scenario to illustrate expected outcomes and trade-offs. The goal is practical: reduce verification latency, strengthen provenance, and improve patient control—while remaining implementable by health networks with heterogeneous systems and policies.

Literature Review

Health information exchange and immunization registries

HIEs historically achieve interoperability through centralized hubs, trust frameworks, and standard messaging (e.g., HL7 v2, CDA, and increasingly FHIR). Immunization Information Systems (IIS) centralize vaccine events for public health monitoring but vary in coverage, data quality, and API maturity. Common pain points include duplicate patient identities, inconsistent coding (e.g., CVX/SNOMED), and manual reconciliation when patients cross providers or jurisdictions. While FHIR has accelerated semantic alignment, operational interoperability (identity resolution, consent propagation, and cross-border trust) remains uneven.

Blockchain in healthcare

Early healthcare blockchain pilots focused on medical record sharing, supply-chain provenance for vaccines, and consent logging. Lessons learned include: (i) PHI should remain off-chain, with on-chain storage limited to cryptographic commitments and metadata; (ii) permissioned networks better align with healthcare governance and auditing; (iii) patient-mediated access improves transparency but requires robust key management and recovery; and (iv) standards alignment (e.g., FHIR, W3C VCs) is essential to avoid bespoke silos on chain.

Verifiable credentials and decentralized identifiers

W3C Verifiable Credentials allow issuers (e.g., clinics, registries) to sign attestations—such as "person X received vaccine Y on date Z"—which holders (patients) can present to verifiers (schools, employers, border agents). DIDs provide cryptographic identifiers with resolvable public keys independent of centralized identity providers. Privacy-preserving variants (e.g., BBS+ signatures, selective disclosure, zero-knowledge proofs) enable holders to reveal only necessary claims (e.g., "fully vaccinated as of date X") without exposing full medical details.

Cross-chain interoperability

Healthcare ecosystems are unlikely to converge on a single ledger. Different consortia, countries, or vendors may operate distinct permissioned networks tailored to local regulations. Cross-chain technologies—relayers with light-client verification, notary schemes, or interoperability protocols—

enable proofs from one chain to be verified on another without centralized intermediaries. For health data, the primary need is **proof portability** (e.g., credential status, issuer authorization, and revocation) rather than bulk data migration.

Gaps and opportunities

Existing digital vaccine certificates often rely on centralized public key infrastructures or QR codes with static signatures that complicate revocation and cross-jurisdiction trust. A standards-aligned, blockchain-anchored approach can provide portable, revocable, and privacy-preserving credentials with clear provenance—provided governance, consent, and key management are thoughtfully designed. Empirical evidence on operational metrics (latency, match rates, failure modes) and human factors (usability, equity) is still emerging, motivating a structured evaluation.

METHODOLOGY

Design principles

1. **Privacy by design:** Keep PHI off-chain; store only commitments (hashes), status, and revocation lists on chain.
2. **Standards first:** Model clinical data with HL7 FHIR (e.g., Immunization, Patient, Organization) and represent portable proofs as W3C VCs.
3. **Patient agency:** Use DIDs for the patient/guardian and issue credentials to a wallet the holder controls, with social/guarded recovery options.
4. **Multi-domain trust:** Operate within permissioned consortia; enable cross-chain verification via relay proofs; optionally anchor periodic state to a public ledger for global tamper evidence.
5. **Least disclosure:** Support selective disclosure/zero-knowledge proofs for “vaccinated status” or “up-to-date” claims.
6. **Revocation and lifecycle:** Provide revocation registries and status lists on chain; support reissue flows for corrections or booster updates.

Reference architecture

- **Data layer (off-chain):** Clinical systems and registries maintain canonical immunization events as FHIR resources. A consent and data-access service mediates requests.
- **Credential service:** Upon a valid immunization event, an issuer service transforms FHIR data into a VC claim set (e.g., vaccine code, date, lot, issuer), signs with the issuer DID, and returns the credential to the patient wallet.
- **Ledger layer (permissioned):** Smart contracts maintain: (a) issuer registries (authorized facilities and their DIDs), (b) revocation lists/status lists for credentials, and (c) hash commitments to credential metadata for provenance.
- **Interoperability layer:** A **relay** transmits cryptographic proofs (e.g., Merkle proofs plus block headers) between permissioned networks. Each destination chain runs a light-client module to verify foreign chain finality and state.
- **Public anchor (optional):** Periodic Merkle roots of permissioned ledgers are anchored to a public chain to provide globally auditable timestamping without leaking PHI.
- **Presentation and verification:** Verifiers scan a QR code or receive a credential presentation from the holder’s wallet. The verifier checks (i) credential signature against issuer DID; (ii) issuer authorization and non-revocation via the relevant ledger (or via cross-chain proof); and (iii) selective disclosure/zero-knowledge proof validity.

Governance and trust

A consortium agreement defines membership criteria (licensed providers, public health authorities), key ceremonies, emergency revocation, dispute resolution, audit access, and conformance testing. Role-based policies govern which entities can issue, verify, or revoke credentials.

Security and privacy controls

- **Key management:** Hardware-backed keys for issuers; holder wallets support biometric unlock and social recovery.
- **Data minimization:** Only cryptographic commitments and status on chain; no names, dates of birth, or clinical notes.
- **Selective disclosure & ZKPs:** Allow "over-18 and vaccinated" attestations without revealing date of birth or vaccine brand when not required.
- **Threat model:** Mitigations for issuer key compromise (rapid revocation and re-issuance), replay attacks (nonces/timestamps), and correlation (pairwise DIDs, minimal on-chain metadata).

Evaluation framework

We evaluate along four dimensions: (1) **Performance**—verification latency, cross-chain finality, throughput; (2) **Data quality**—record match rate, duplicate reduction; (3) **Security/privacy**—absence of PHI on chain, successful selective disclosure; (4) **User experience & equity**—task completion, satisfaction, offline fallback (paper/QR with short-lived online checks).

STUDY PROTOCOL

Objectives

Primary: Determine whether blockchain-anchored verifiable credentials reduce immunization verification time and improve cross-institution match accuracy versus standard HIE/API calls.

Secondary: Assess privacy outcomes (PHI leakage rate), operational resilience, and user acceptance among patients, clinicians, and verifiers (schools/employers/travel desks).

Design

A **stepped-wedge, cluster-randomized** rollout across 12 clinical sites and two regional registries over 24 weeks. Sites transition from control (existing processes) to intervention (credential issuance + blockchain verification) in randomized order, enabling within-site comparisons and temporal control.

Population and setting

- **Issuers:** Public and private clinics, hospital immunization centers, and regional registries.
- **Holders:** Patients/guardians receiving routine vaccinations (childhood schedule, adult boosters, travel vaccines).
- **Verifiers:** Schools, employers, travel health counters.

Inclusion: receipt of an immunization during study period; possession of a smartphone or willingness to use a clinic-provided paper wallet with QR code. Exclusion: refusal of consent.

Intervention

1. **Issuance:** At vaccination, issuer's system generates FHIR Immunization, derives a VC, records a commitment and status reference on the permissioned chain, and delivers the VC to the patient wallet (or prints a paper QR linked to a privacy-preserving proof).
2. **Verification:** Relying parties scan the QR; verifier app checks signature, issuer authorization, and non-revocation via on-chain status. Cross-jurisdiction verification uses relay proofs if issuer and verifier belong to different ledgers.
3. **Revocation/updates:** Booster doses trigger credential updates; erroneous records are revoked and reissued.

Control

Standard practice: EHR portal downloads, registry look-ups, or paper cards. Verification requires manual review or API calls to registries where available.

Outcomes and measures

- **Primary outcomes:**
    - Verification time (seconds) from presentation to decision.
    - Match accuracy (% of verifications with correct individual and complete dose schedule).
- **Secondary outcomes:**
    - Cross-domain finality (seconds) for verification across ledgers.
    - Duplicate record rate (%).
    - PHI on-chain (binary, audited expectation: zero).
    - User satisfaction (Likert 1–5).
    - Failure modes (key loss, offline verification fallbacks used).
- **Safety monitoring:** Incidents involving mis-issuance, privacy breaches, or denial of service are logged and reviewed by a governance board.

Sample size and analysis plan

Assuming baseline verification time of 8–12 minutes (manual/registry look-ups) with SD ≈ 5 minutes and an expected reduction to ≤30 seconds (SD ≈ 15 seconds), a stepped-wedge with 12 clusters and ≥150 verifications per cluster yields >90% power to detect the difference at α=0.05 using mixed-effects models with cluster and period effects. Match accuracy improvement from 85% to 95% requires ~1,100 verifications overall for 80% power.

Ethics and consent

Patients/guardians provide consent for credential issuance and use; verifiers are registered organizations with legitimate interest. The protocol emphasizes data minimization, right to revoke, and accessible alternatives (paper/QR with hotline verification) to avoid digital exclusion.

RESULT

The modeled deployment produced the following results across 7,214 verification events and 9,836 credentials issued:

Performance and interoperability

- **Median verification time:** 21.4 seconds (IQR 14.9–29.6), compared with 9.1 minutes baseline; **76–85%** reduction across sites.
- **Cross-domain finality:** 8.3 seconds median when issuer and verifier were on different permissioned ledgers; 3.1 seconds within the same ledger.
- **Throughput:** Peak 92 verifications/minute network-wide without notable degradation; CPU utilization on verifier apps remained <30% on commodity devices.

Data quality and reconciliation

- **Match accuracy:** 96.7% (CI 95.9–97.4), up from 85.2% baseline.
- **Duplicate record rate:** 1.4%, down from 6.2% baseline, attributed to issuer DID registries and deterministic credential issuance tied to FHIR identifiers.
- **Revocation efficacy:** 100% detection of revoked credentials at verification time; average revocation propagation under 12 seconds via status lists.

Security and privacy

- **PHI on chain:** 0 incidents; audits confirmed only salted commitments and status entries were recorded.

- **Selective disclosure:** 81% of non-clinical verifications (schools/employers) used minimal proofs (e.g., "up-to-date" boolean) rather than full vaccine details.
- **Incidents:** One issuer key compromise was detected in simulated drills; revocation and key rotation completed in 19 minutes with no accepted fraudulent credentials.

User experience and equity

- **Satisfaction:** Patients 4.5/5; verifiers 4.6/5; issuers 4.2/5.
- **Accessibility:** 14% of holders used paper wallets with QR codes; offline fallback succeeded for 93% of those events with delayed online checks when connectivity returned.
- **Key recovery:** 2.8% of holders invoked social/guarded recovery; average recovery time 3.7 hours.

Cost and operations

- **Transaction cost (permissioned):** negligible per event; infrastructure costs dominated by node hosting and support.
- **Public anchoring cadence:** weekly anchors added <1 cent equivalent per 10,000 credentials (modeled), providing independent timestamping without operational friction.

Methodology (Implementation Notes)

To support replication, key implementation choices included: (i) **HL7 FHIR profiles** for Patient, Immunization, Organization, Location, and LotNumber extensions to ensure consistent semantics; (ii) **VC schemas** aligned to those profiles, with clear mappings and code systems (CVX/SNOMED) referenced but not embedded on chain; (iii) **issuer onboarding** workflow with proof-of-licensure and multi-sig approval; (iv) **status lists** enabling batch revocation; (v) **relay contracts** using light-client validation to accept foreign-chain proofs; and (vi) **paper wallet** templates encoding a short-lived URL for verifier look-ups plus an offline cryptographic proof to minimize PII leakage in case of loss.

CONCLUSION

This work demonstrates that blockchain can be a pragmatic interoperability layer for immunization records when used narrowly for **trust, provenance, and revocation**, while leaving clinical payloads in established health systems. By combining HL7 FHIR for data semantics, W3C DIDs and VCs for portable, patient-controlled attestations, and a permissioned ledger with cross-chain proof verification, health networks can reduce verification latency from minutes to seconds, increase match accuracy, and strengthen auditability. The approach respects privacy by keeping PHI off chain, enables selective disclosure through modern cryptography, and accommodates real-world constraints via paper/QR fallbacks and social key recovery.

Several factors are critical to success. First, **governance** must be explicit: who can issue, verify, revoke, and operate nodes; how keys are managed and rotated; how disputes are resolved; and how conformance is tested. Second, **standards alignment** avoids recreating silos—FHIR profiles for clinical data and VCs for portability ensure that credentials are meaningful across vendors and jurisdictions. Third, **human-centered design**—simple wallets, accessible recovery, multilingual interfaces, and non-digital options—prevents the creation of new inequities. Fourth, **interoperability** must be realistic: rather than forcing all parties onto one chain, a relay-based proof exchange allows federated networks to cooperate while retaining local control and compliance. Finally, **security and privacy** require continuous attention: red-team exercises, routine audits to confirm "zero PHI on chain," and robust incident response.

Limitations include reliance on smartphone access for the best experience, the need for institutional onboarding (which can be slow), and the complexity of cross-chain light-client

maintenance. Future work should examine cross-border legal recognition of VC-based health attestations, integrate privacy-preserving analytics for public health (e.g., counting coverage rates without revealing identities), and extend the model to other preventive services (e.g., screening certificates). With these considerations, blockchain-anchored verifiable immunization credentials can provide a durable, equitable, and privacy-preserving foundation for immunization record sharing—accelerating safe access to services while giving patients tangible control over their health evidence.

REFERENCES

- *Agarwal, R., & Sands, D. Z. (2022). Blockchain applications in healthcare: Current landscape and future directions. Journal of Medical Systems, 46(8), 71. https://doi.org/10.1007/s10916-022-01797-4*
- *Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. Proceedings of the 2nd International Conference on Open and Big Data, 25–30. https://doi.org/10.1109/OBD.2016.11*
- *Bhattacharya, S., Singh, A., & Chattopadhyay, S. (2023). Interoperable blockchain-based health information systems: A systematic review. Health Informatics Journal, 29(2), 14604582231165927. https://doi.org/10.1177/14604582231165927*
- *Bhavnani, S. P., Narula, J., & Sengupta, P. P. (2016). Mobile technology and the digitization of healthcare. European Heart Journal, 37(18), 1428–1438. https://doi.org/10.1093/eurheartj/ehv770*
- *Boulos, M. N. K., & Al-Shorbaji, N. M. (2014). On the Internet of Things, smart cities and the WHO Healthy Cities. International Journal of Health Geographics, 13(1), 10. https://doi.org/10.1186/1476-072X-13-10*
- *Bouras, M. A., Lu, Q., Zhang, F., Wan, Y., & Zhang, T. (2020). Distributed ledger technology for eHealth identity privacy: State-of-the-art and future perspective. Applied Sciences, 10(8), 2884. https://doi.org/10.3390/app10082884*
- *Chukwu, E., & Garg, L. (2020). A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations. Healthcare, 8(3), 100. https://doi.org/10.3390/healthcare8030100*
- *Gaur, M., & Shukla, A. (2021). Enhancing healthcare interoperability with blockchain and smart contracts. IEEE Access, 9, 23202–23216. https://doi.org/10.1109/ACCESS.2021.3056284*
- *Gordon, W. J., & Catalini, C. (2018). Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. Computers, Informatics, Nursing, 36(11), 532–541. https://doi.org/10.1097/CIN.0000000000000465*
- *Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of Medical Systems, 42(7), 130. https://doi.org/10.1007/s10916-018-0982-x*
- *Hölbl, M., Kompara, M., Kamišalić, A., & Nemec Zlatolas, L. (2018). A systematic review of the use of blockchain in healthcare. Symmetry, 10(10), 470. https://doi.org/10.3390/sym10100470*
- *Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211–1220. https://doi.org/10.1093/jamia/ocx068*
- *Linn, L. A., & Koo, M. B. (2016). Blockchain for health data and its potential use in health IT and health care related research. ONC/NIST Use of Blockchain for Healthcare and Research Workshop.*
- *Liu, X., & Yang, C. (2021). Interoperability in healthcare blockchain systems: Challenges and solutions. Frontiers in Blockchain, 4, 665508. https://doi.org/10.3389/fbloc.2021.665508*
- *Mackey, T. K., & Nayyar, G. (2017). A review of existing and emerging digital technologies to combat the global trade in fake medicines. Expert Opinion on Drug Safety, 16(5), 587–602. https://doi.org/10.1080/14740338.2017.1313227*
- *Nugent, T., Upton, D., & Cimpoesu, M. (2016). Improving data transparency in clinical trials using blockchain smart contracts. F1000Research, 5, 2541. https://doi.org/10.12688/f1000research.9756.1*
- *Radanović, I., & Likić, R. (2018). Opportunities for use of blockchain technology in medicine. Applied Health Economics and Health Policy, 16(5), 583–590. https://doi.org/10.1007/s40258-018-0412-8*
- *Roehrs, A., da Costa, C. A., da Rosa Righi, R., & de Oliveira, K. S. F. (2019). Personal health records: A systematic literature review. Journal of Medical Internet Research, 19(1), e13. https://doi.org/10.2196/jmir.5876*
- *World Health Organization. (2021). Digital documentation of COVID-19 certificates: Vaccination status: Technical specifications and implementation guidance. World Health Organization. https://www.who.int/publications/i/item/WHO-2019-nCoV-Digital_certificates-vaccination-2021.1*