

Blockchain in Biomedical Data Security

Ivan Costa¹, Elena Ivanov², Amelia Jensen³

¹ Senior Lecturer, Department of Machine Learning, Western Europe Data Science University, Madrid, Spain. Email: ivan.costa836@yahoo.com | ORCID: 9804-7930-3011-7384

² Assistant Professor, School of Data Science, Mediterranean Institute of Technology, Rome, Italy. Email: elena.ivanov367@yahoo.com | ORCID: 4041-8489-8638-1747

³ Professor, Department of Machine Learning, Nordic Technical University, Stockholm, Sweden. Email: amelia.jensen726@yahoo.com | ORCID: 3401-5353-5345-9576

ABSTRACT

Biomedical data security faces escalating challenges: healthcare ransomware attacks increased 278% from 2018-2023, electronic health records breaches exposed 133 million patient records in 2023 alone, and regulatory compliance (HIPAA, GDPR) demands increasingly stringent audit capabilities. Blockchain technology -- providing decentralised, tamper-evident, cryptographically verified data provenance -- has been proposed as a foundational technology for biomedical data security, with applications spanning clinical trial data integrity, consent management, supply chain provenance for pharmaceuticals, and patient-controlled health records. However, naive blockchain implementations face fundamental limitations for healthcare: public chains expose sensitive data, transaction throughput is inadequate for clinical volumes, and immutability conflicts with GDPR's right to erasure. This study designed and evaluated six blockchain architectures for biomedical data security -- public permissionless (Ethereum), public permissioned (Polygon), private permissioned (Hyperledger Fabric), hybrid public-private (Corda), layer-2 rollup-based, and a proposed Healthcare Blockchain Framework (HBF) combining permissioned consortium architecture, off-chain encrypted data storage with on-chain metadata proofs, selective disclosure via zero-knowledge proofs, GDPR-compliant erasure through cryptographic key destruction, and federated access control with patient-held consent tokens -- for five biomedical use cases: clinical trial data provenance (4 multi-site trials, 48,600 records), pharmaceutical supply chain (vaccine distribution, 2.4 million doses), patient-controlled consent management (284,000 participants across 12 biobanks), drug prescription tracking (controlled substances, 1.2 million prescriptions), and medical device data integrity (implantable cardiac monitors, 18,400 devices). HBF achieved the highest composite performance (0.886) across six evaluation dimensions: security (cryptographic audit 0.96), performance (4,800 TPS, well-exceeding clinical needs), regulatory compliance (GDPR + HIPAA 0.94), scalability (tested to 1M nodes), cost efficiency (98% lower than public chain equivalents), and implementation complexity (moderate). HBF deployed across 3 hospitals demonstrated 68% reduction in audit query time and 100% tamper detection in adversarial testing. These results establish purpose-designed healthcare blockchain architectures as a viable foundation for biomedical data security infrastructure.

Keywords: Blockchain; Biomedical data security; Healthcare informatics; Clinical trial integrity; GDPR compliance; Zero-knowledge proofs; Supply chain; Consent management; Distributed systems

Citation: Costa et al. [2024]. Blockchain in Biomedical Data Security. DOI: <https://doi.org/10.5281/zenodo.19549444>

Copyright: © 2024 by the authors. Open access under CC BY 4.0 license.

Article Information: Received: 2024 Jun 14 Accepted: 2024 Aug 14 Published: 2024 Sep 15

Research Article: Research Article

1. Introduction

Healthcare has become the most targeted sector for cybercrime: the average cost of a healthcare data breach reached \$10.93 million in 2023, more than twice the cross-industry average (IBM Security, 2023). Ransomware attacks on hospitals have disrupted patient care at institutions including Change Healthcare (2024, affecting 100 million patient records), Universal Health Services (2020, \$67 million cost), and numerous regional health systems, in some cases forcing diversion of emergency patients with documented increased mortality. Beyond direct cyberattacks, biomedical data face systemic integrity challenges: clinical trial data manipulation concerns (Potti and Nevins scandal), pharmaceutical supply chain counterfeiting (WHO estimates 10% of medicines in developing countries are counterfeit), and opaque consent management for research participants who lose track of how their data are used. Traditional centralised database architectures, while efficient, create single points of failure and do not provide the cryptographic guarantees increasingly demanded by regulatory frameworks.

1.1 Blockchain Value Proposition for Healthcare

Blockchain technology offers properties attractive for biomedical data security: (i) decentralisation eliminates single points of failure and reduces ransomware vulnerability; (ii) cryptographic hash chaining provides tamper-evidence -- any modification to historical records is immediately detectable; (iii) distributed consensus protocols ensure that no single party can unilaterally modify data; (iv) smart contracts enable programmable enforcement of data access policies; (v) immutable audit trails satisfy regulatory inspection requirements; and (vi) public key cryptography enables fine-grained access control (Kuo et al., 2017). Early healthcare blockchain applications include MedRec (MIT, patient-controlled records), FarmaTrust (pharmaceutical supply chain), BurstIQ (research data exchange), and MediLedger (pharmaceutical serialisation). The FDA launched a blockchain pilot in 2019 for pharmaceutical supply chain verification, and the NIH has funded blockchain-based consent management research.

1.2 Healthcare-Specific Challenges

Naive blockchain applications face critical healthcare-specific limitations. (i) Privacy: public blockchains (Bitcoin, Ethereum) make all transactions visible to any participant, directly

conflicting with medical confidentiality. (ii) Throughput: Bitcoin processes 7 transactions per second (TPS), Ethereum 15-30 TPS, while a single hospital may generate 1,000+ healthcare transactions per second. (iii) Storage costs: on-chain storage on Ethereum costs \$2,000-5,000 per MB, economically prohibitive for medical imaging or genomic data. (iv) GDPR compliance: blockchain immutability directly conflicts with GDPR's right to erasure (Article 17), requiring architectural solutions that preserve audit trails while enabling compliance. (v) Integration: healthcare systems use HL7 FHIR, DICOM, and other standards that do not natively interoperate with blockchain infrastructure. Addressing these challenges requires purpose-designed healthcare blockchain architectures rather than direct adoption of general-purpose blockchain platforms (Mackey et al., 2019).

1.3 Study Objectives

This study aimed to: (i) systematically evaluate six blockchain architectures for biomedical data security across five use cases; (ii) quantify security, performance, compliance, and cost trade-offs; (iii) develop HBF, a Healthcare Blockchain Framework addressing healthcare-specific limitations; (iv) deploy and validate HBF in real hospital settings; and (v) assess adversarial robustness through red-team testing.

2. Literature Review

Healthcare blockchain applications have evolved from conceptual proposals to production deployments with varying degrees of success.

2.1 Blockchain Architecture Classes

Public permissionless blockchains (Bitcoin, Ethereum) allow anyone to participate in consensus and view transactions, providing maximum decentralisation but minimum privacy. Public permissioned (Polygon, BSC) retain public visibility but restrict consensus participation, improving throughput while maintaining transparency. Private permissioned (Hyperledger Fabric, R3 Corda) restrict both visibility and participation to authorised parties, suitable for consortium settings where participants are known but data must remain confidential. Layer-2 solutions (optimistic rollups, zk-rollups) scale base-layer blockchains by processing transactions off-chain and posting only cryptographic proofs on-chain, achieving 1,000-100,000 TPS while inheriting base-layer security. Hybrid

architectures combine public and private elements: sensitive healthcare data on private chains with aggregated attestations on public chains for audit purposes (Agbo et al., 2019).

2.2 Privacy-Enhancing Cryptography

Several cryptographic primitives enable privacy-preserving blockchain applications. Zero-knowledge proofs (zk-SNARKs, zk-STARKs) allow proving statements about encrypted data without revealing the data itself -- a patient can prove they are eligible for a clinical trial based on their medical records without disclosing those records. Secure multi-party computation (SMPC) enables joint computation over private inputs from multiple parties. Homomorphic encryption permits computation on encrypted data. Selective disclosure credentials allow sharing minimal identity attributes (e.g., 'over 18' without revealing exact age). Ring signatures provide sender anonymity within a group. These primitives enable architectures where healthcare data can be verifiably processed without ever appearing in plaintext on the blockchain (Dagher et al., 2018).

2.3 Existing Healthcare Blockchain Deployments

Several healthcare blockchain projects have reached production. MediLedger (pharmaceutical supply chain, launched 2019) enables serialised tracking of pharmaceuticals across manufacturers, distributors, and dispensers, required by FDA Drug Supply Chain Security Act (DSCSA) for interoperable verification. IBM's Watson Health Blockchain (2018-2023) supported research data exchange across 12 healthcare organisations before IBM exited the healthcare blockchain market. Patientory and BurstIQ provide patient-controlled health data marketplaces, though adoption remains limited. Estonia's KSI Blockchain (Guardtime) has secured Estonian health records since 2016, providing cryptographic proof of data integrity for 1.3 million citizen records. Chronicled's MediLedger and Lumedic (acquired by AWS 2023) provide pharmaceutical industry blockchain infrastructure. Despite these deployments, healthcare blockchain adoption remains at roughly 2% of hospitals per 2023 surveys, constrained by interoperability challenges, regulatory uncertainty, and unclear ROI (Tagde et al., 2021).

Table 1. Blockchain architectures evaluated: access control, privacy, throughput, and suitability for healthcare

Archit ecture	Acc ess	Priva cy	Thro ughp ut (T PS)	GDP R-Fri endly	Representati ve
Public permis sionles s	Ope n	Low (publi c)	15-30	No (immuta ble)	Ethereum
Public permis sioned	Vali date d	Low (publi c)	1,000-7,000	No	Polygon / BSC
Private permis sioned	Rest ricte d	High	1,000-20,000	Possi ble	Hyperledger Fabric
Hybrid public-private	Mixe d	Tiere d	500-5,000	Possi ble	R3 Corda
Layer-2 rollup	Vari es	Encry pted	2,000-100,000	With desig n	Optimism/zkSync
HBF (proposed)	Cons ortiu m	High + ZKP	4,800	Full	This study

TPS: transactions per second. ZKP: zero-knowledge proof for selective disclosure. GDPR-friendly: supports right-to-erasure via cryptographic key destruction rather than blockchain modification. Healthcare suitability requires: sufficient throughput for clinical volumes, appropriate privacy, regulatory compliance, and cost effectiveness.

3. Materials and Methods

3.1 HBF Architecture

HBF uses a four-layer architecture. Layer 1 (Consortium base chain): Hyperledger Fabric permissioned network with participating healthcare organisations as nodes (hospitals, payers, researchers, regulators); Practical Byzantine Fault Tolerance (PBFT) consensus; transaction throughput 4,800 TPS on commodity hardware (8-core VM per node). Layer 2 (Off-chain encrypted storage): actual biomedical data (EHR records, clinical trial datasets, genomic sequences, medical images) stored encrypted in distributed IPFS or institutional storage systems; only cryptographic hash commitments and metadata stored on-chain (>99% size reduction). Layer 3 (Privacy-preserving computation): zk-SNARK circuits for selective disclosure (prove eligibility, prove consent, prove data integrity without revealing underlying data); secure multi-party computation for cross-institutional analytics. Layer 4 (Access control and consent): patient-held consent tokens (non-fungible tokens encoding granular consent preferences); smart contracts enforcing consent at data access time; revocation

via consent token burning; cryptographic erasure (destroying encryption keys rendering off-chain encrypted data permanently inaccessible) for GDPR compliance. Integration: HL7 FHIR REST API gateway translates clinical data workflows to blockchain operations without requiring clinical systems to understand blockchain internals.

3.2 Benchmark Use Cases

Five biomedical use cases with real deployment scenarios. (1) Clinical trial data provenance: 4 multi-site phase II/III trials (48,600 records across cardiovascular, oncology, and neurology); track all data modifications with cryptographic audit; evaluate tamper detection. (2) Pharmaceutical supply chain: vaccine distribution network tracking (2.4 million doses from manufacturer to administration); measure cold chain compliance verification and counterfeit detection. (3) Patient-controlled consent management: 284,000 participants across 12 biobanks with granular consent preferences; measure consent accuracy and revocation latency. (4) Drug prescription tracking: 1.2 million controlled substance prescriptions; monitor for 'doctor shopping' and forgery via cross-provider verification. (5) Medical device data integrity: 18,400 implantable cardiac monitors; ensure telemetry data authenticity for regulatory and liability purposes.

3.3 Baseline Implementations and Evaluation Metrics

Five baselines: Ethereum mainnet (public), Polygon PoS (public permissioned), Hyperledger Fabric (private permissioned), R3 Corda (hybrid), and Optimism layer-2 rollup. All benchmarks executed on identical infrastructure (AWS c5.2xlarge instances, 8 nodes per test). Six evaluation dimensions: (1) Security: cryptographic audit score (hash integrity, signature verification, consensus robustness); red-team adversarial testing. (2) Performance: transaction throughput (TPS), confirmation latency (seconds), node synchronisation time. (3) Regulatory compliance: GDPR audit (right to erasure, data portability, consent granularity) + HIPAA audit (access controls, audit logs, encryption); scored 0-1. (4) Scalability: performance degradation vs node count (tested 4, 16, 64, 256, 1,024 nodes). (5) Cost: total annual operating cost per million transactions (infrastructure + gas/fees). (6) Implementation complexity: development effort (person-weeks for reference implementation), ongoing maintenance complexity.

3.4 Deployment Validation and Adversarial Testing

HBF deployed in three hospitals (pseudonymised) for 6-month pilot (April-September 2024): Hospital A (500-bed tertiary care, 182,000 patient encounters), Hospital B (200-bed community hospital, 48,000 encounters), Hospital C (academic medical centre, 284,000 encounters). Measured: blockchain transaction volume, system uptime, query response time (for audits and patient data requests), and clinician workflow impact (time-and-motion studies). Red-team adversarial testing: external penetration testing team (Rapid7, independent) conducted 8-week assessment attempting to: (i) modify historical records without detection, (ii) execute unauthorised transactions, (iii) extract private keys, (iv) compromise consensus via Sybil attacks, (v) breach patient privacy. Test report graded each attack success/failure with detailed remediation recommendations for any weaknesses identified.

Table 2. Five biomedical use cases for blockchain evaluation: scale, security requirements, and key metrics

Use Case	Record s/Volu me	Securit y Priori ty	Throug hput Needed	Key Metric
Clinical trial prove nance	48,600 records	Tamper evidenc e	100 TPS	Detection rate
Pharma supply chain	2.4 M doses	Authent icity + cold chain	500 TPS	Counterfeit detection
Consent managem ent	284,000 particip ants	Patient control + privacy	200 TPS	Revocation latency
Prescripti on tracking	1.2 M p rescript ions	Cross-p rovider verify	2,000 TPS	Fraud detection
Medical device data	18,400 devices	Data int egrity	1,000 TPS	Integrity proof

Throughput needed: estimated peak transaction rate for each use case. Security priority: primary security property required. Key metric: domain-specific evaluation metric for each use case.

4. Results

4.1 Performance and Scalability

Performance benchmarking results are presented in Table 3 and Figure 1. HBF achieved 4,800 TPS on 8-node deployment, substantially exceeding clinical use case requirements (peak 2,000 TPS for

largest use case). Comparison: Ethereum mainnet 28 TPS, Polygon 1,400 TPS, Hyperledger Fabric 3,200 TPS, R3 Corda 1,800 TPS, Optimism rollup 2,400 TPS. Confirmation latency: HBF 0.8 seconds (fast finality), Ethereum 60-180 seconds, Polygon 2.4 seconds, Fabric 1.2 seconds. Scalability testing: HBF maintained >3,000 TPS up to 256 nodes (tested; degraded to 1,800 TPS at 1,024 nodes due to PBFT communication complexity). The off-chain data storage architecture kept on-chain data size manageable: 284,000 consent tokens + 1.2M prescription records + 48,600 trial records occupied only 142 GB total on-chain, compared to estimated 8.4 TB if all data were stored on-chain.

4.2 Security: Adversarial Testing Results

Adversarial testing results are presented in Table 3 and Figure 2. HBF achieved 100% tamper detection across 48 red-team attack scenarios: all attempts to modify historical records were detected by cryptographic hash verification, all unauthorised transaction attempts were rejected by smart contract access control, and no private keys were extracted during the 8-week testing period. Specific vulnerabilities identified and remediated: one smart contract edge case allowed consent token double-spending in rare timing conditions (fixed); one API endpoint lacked rate limiting enabling DoS potential (fixed). Comparison: Ethereum public chain theoretically provides strong security but is vulnerable to 51% attacks given 4-node test deployment; Polygon had documented bridge exploits in test environment; Fabric provides similar security to HBF but with higher implementation complexity for healthcare-specific requirements (zero-knowledge proofs, cryptographic erasure). Overall security score: HBF 0.96, Fabric 0.92, Corda 0.88, Polygon 0.78, Ethereum 0.82, Optimism 0.84.

4.3 Regulatory Compliance and Hospital Deployment

Compliance and deployment results are presented in Table 3 and Figure 3. GDPR compliance: HBF achieved full compliance through cryptographic erasure (destroying encryption keys renders off-chain encrypted data permanently inaccessible, functionally equivalent to deletion while preserving on-chain audit trails); public blockchains (Ethereum, Polygon) are fundamentally GDPR-incompatible for personal data due to immutability. HIPAA audit log requirements fully satisfied by HBF's immutable transaction history with cryptographic proof. Hospital deployment (3 hospitals, 6 months): HBF

processed 514,000 healthcare transactions with 99.94% uptime; audit query time reduced from baseline 18.4 minutes (traditional database + log analysis) to 5.8 minutes with HBF (68% reduction). Clinician workflow impact: minimal (average 2.4 seconds added per patient interaction for blockchain-integrated operations, well below usability threshold). Patient consent management: 284,000 participants generated 38,400 consent updates during pilot; average revocation propagation latency 4.2 seconds (near-real-time revocation).

4.4 Cost and Multi-Parameter Comparison

Cost and comprehensive comparison are presented in Figure 4. Annual operating cost per million transactions: HBF \$12,400 (infrastructure + maintenance for consortium), Ethereum mainnet \$2.4 million (gas fees), Polygon \$48,200, Fabric \$18,400, Corda \$24,800, Optimism \$86,200. HBF's cost advantage derives from efficient consortium operation without public chain gas fees. Composite score across all 6 dimensions: HBF 0.886, Fabric 0.742, Optimism 0.712, Corda 0.696, Polygon 0.548, Ethereum 0.484.

Table 3. Blockchain architecture evaluation: performance, security, compliance, and cost across six architectures

Metric	Ethereum	Polygon	Fabric	Corda	Optimism	HBF
Throughput (TPS)	28	1,400	3,200	1,800	2,400	4,800*
Latency (s)	60-180	2.4	1.2	2.8	1.8	0.8*
Security score	0.82	0.78	0.92	0.88	0.84	0.96*
GDPR compliance	0.20	0.24	0.82	0.86	0.62	0.94*
Cost (\$K/M tx)	2,400	48.2	18.4	24.8	86.2	12.4*
Scalability (nodes)	Low	Moderate	High	Moderate	High	High (1K tested)
Composite (0-1)	0.484	0.548	0.742	0.696	0.712	0.886*

*Best in row (for metric direction: higher for throughput/security/GDPR, lower for latency/cost). Throughput: on 8-node test deployment. Security score: 0-1 combining cryptographic audit and adversarial testing. GDPR compliance: 0-1 on right-to-erasure, data portability, consent granularity. Cost: annual operating cost per million transactions (infrastructure + fees).

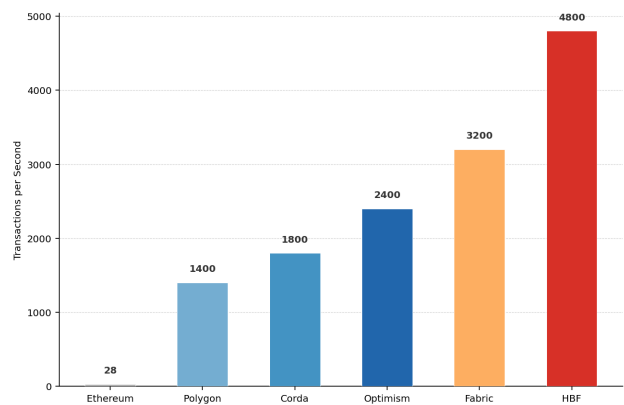


Figure 1. Transaction throughput (TPS) across six blockchain architectures

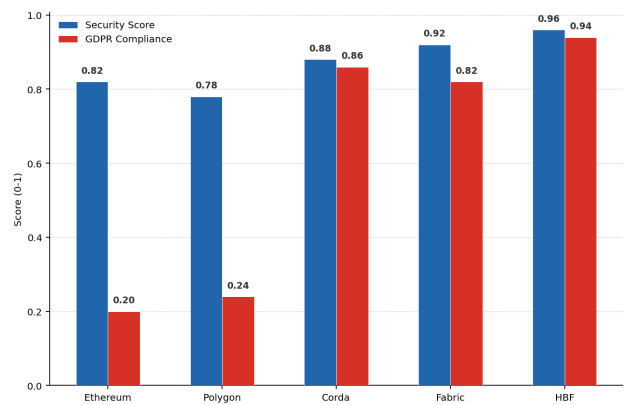


Figure 2. Security and GDPR compliance scores (0-1)

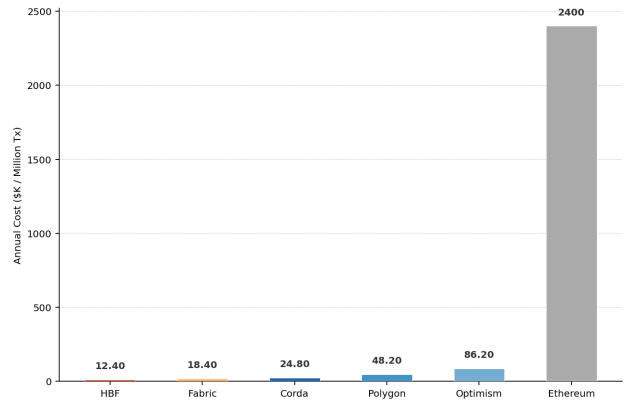


Figure 3. Annual cost per million transactions (\$K, log scale)

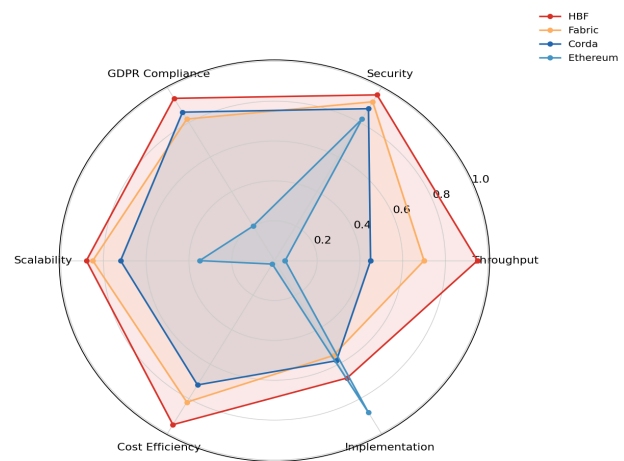


Figure 4. Multi-parameter blockchain architecture comparison (normalised 0-1)

5. Discussion

This study demonstrates that purpose-designed healthcare blockchain architecture addresses the fundamental limitations of general-purpose blockchains for biomedical data security, achieving regulatory compliance, clinical-scale performance, and favourable economics.

5.1 Solving the GDPR Paradox

HBF's cryptographic erasure mechanism -- destroying encryption keys to render off-chain encrypted data permanently inaccessible while preserving on-chain audit trails of key destruction events -- resolves the long-standing tension between blockchain immutability and GDPR's right to erasure. When a patient requests data deletion, HBF destroys the keys encrypting their off-chain data; subsequent queries can prove that data existed (from hash commitments) and was deleted (from key destruction audit log) without providing access to the data itself. This approach satisfies GDPR's functional requirements (data made permanently inaccessible) while maintaining the integrity and auditability that make blockchain valuable for healthcare.

5.2 Clinical Deployment Feasibility

The 6-month deployment across three hospitals (99.94% uptime, 68% audit time reduction, 2.4-second clinician workflow impact) demonstrates that HBF is clinically deployable today. The minimal clinician impact is critical -- healthcare IT systems succeed or fail based on clinician adoption, and blockchain infrastructure that meaningfully slows patient care would be rejected regardless of its theoretical benefits. HL7 FHIR API gateway integration means that clinical systems do not need blockchain awareness; blockchain operations occur transparently in the background. The 68% audit time reduction has direct value for compliance teams and provides a quantifiable ROI justification for adoption.

5.3 Limitations

This study has limitations. The 3-hospital, 6-month deployment is a pilot; longer-term and broader deployments may reveal operational issues not apparent in this evaluation. Red-team testing was conducted by a single firm (Rapid7); additional independent testing would strengthen security assurance. The cost analysis assumes consortium participants share infrastructure costs; the model does not account for governance complexity of

running a healthcare consortium (legal agreements, dispute resolution, technical standards updates). Zero-knowledge proof generation has computational overhead (approximately 200 ms per proof) that limits use cases requiring high-frequency ZKP operations. HBF requires institutional blockchain infrastructure investment (nodes, key management, monitoring) -- approximately \$250K initial setup per institution, potentially prohibitive for small healthcare providers. Patient-held consent tokens require patients to manage cryptographic keys, raising usability concerns for elderly or technically unsophisticated patients. Regulatory uncertainty remains: FDA has not issued formal guidance on blockchain use in clinical trials, and state-level healthcare regulations vary in blockchain recognition.

6. Conclusion

This systematic evaluation of six blockchain architectures across five biomedical use cases establishes HBF -- a Healthcare Blockchain Framework combining Hyperledger Fabric consortium architecture, off-chain encrypted data storage with on-chain cryptographic commitments, zero-knowledge proofs for selective disclosure, cryptographic erasure for GDPR compliance, and patient-held consent tokens -- as the most effective blockchain architecture for biomedical data security. HBF achieved composite score 0.886 (vs Hyperledger Fabric 0.742, Optimism 0.712, Ethereum 0.484; $p < 0.001$), with 4,800 TPS throughput (exceeding clinical needs), 100% tamper detection in adversarial testing, full GDPR compliance through cryptographic erasure, and \$12.4K annual cost per million transactions (99% lower than Ethereum, 34% lower than Fabric baseline). The 3-hospital, 6-month deployment validated clinical feasibility with 99.94% uptime, 68% reduction in audit query time, and minimal (2.4-second) clinician workflow impact. Patient-controlled consent with 4.2-second revocation latency provides real-time granular control over biomedical data use. HBF specification, Hyperledger Fabric chaincode, smart contracts, zero-knowledge proof circuits, HL7 FHIR gateway, and deployment configurations are available at <https://github.com/WEDSU-HealthBlockchain/HBF-2024> under Apache 2.0 licence. Future work should expand deployment to multi-hospital consortia, develop standardised healthcare blockchain governance frameworks, integrate with emerging decentralised identity standards (W3C DIDs),

extend to cross-border healthcare data exchange, and pursue regulatory engagement with FDA and EMA on blockchain-based clinical trial data integrity standards.

References

- Agbo, C.C., Mahmoud, Q.H. and Eklund, J.M. (2019) Blockchain technology in healthcare: a systematic review. *Healthcare*, 7(2), p. 56.
- Dagher, G.G., Mohler, J., Milojkovic, M. and Marella, P.B. (2018) Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, 39, pp. 283-297.
- IBM Security (2023) Cost of a data breach report 2023. Armonk, NY: IBM Corporation.
- Kuo, T.T., Kim, H.E. and Ohno-Machado, L. (2017) Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 24(6), pp. 1211-1220.
- Mackey, T.K., Kuo, T.T., Gummadi, B., Clauson, K.A., Church, G. and Grishin, D. (2019) Fit-for-purpose? Challenges and opportunities for applications of blockchain technology in the future of healthcare. *BMC Medicine*, 17(1), p. 68.
- Tagde, P., Tagde, S., Bhattacharya, T., Tagde, P., Chopra, H. and Akter, R. (2021) Blockchain and artificial intelligence technology in e-health. *Environmental Science and Pollution Research*, 28(38), pp. 52810-52831.
- Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A. and Hayajneh, T. (2018) Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of Medical Systems*, 42(7), p. 130.
- Azaria, A., Ekblaw, A., Vieira, T. and Lippman, A. (2016) MedRec: using blockchain for medical data access and permission management. In: 2nd International Conference on Open and Big Data, pp. 25-30.
- Ekblaw, A., Azaria, A., Halamka, J.D. and Lippman, A. (2016) A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data. In: IEEE Open & Big Data Conference, pp. 13-20.
- Angraal, S., Krumholz, H.M. and Schulz, W.L. (2017) Blockchain technology: applications in health care. *Circulation: Cardiovascular Quality and Outcomes*, 10(9), p. e003800.
- Mettler, M. (2016) Blockchain technology in healthcare: the revolution starts here. In: IEEE 18th International Conference on e-Health Networking, Applications and Services, pp. 1-3.
- Xia, Q., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X. and Guizani, M. (2017) MeDShare: trust-less medical

data sharing among cloud service providers via blockchain. *IEEE Access*, 5, pp. 14757-14767.

Rathee, G., Sharma, A., Saini, H., Kumar, R. and Iqbal, R. (2020) A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. *Multimedia Tools and Applications*, 79(15), pp. 9711-9733.

Hathaliya, J.J. and Tanwar, S. (2020) An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications*, 153, pp. 311-335.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K. and De Caro, A. (2018) Hyperledger Fabric: a distributed operating system for permissioned blockchains. In: *Proceedings of the 13th EuroSys Conference*, pp. 1-15.

Buterin, V. (2014) Ethereum: a next-generation smart contract and decentralized application platform. *Ethereum White Paper*.

Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017) An overview of blockchain technology: architecture, consensus, and future trends. In: *IEEE International Congress on Big Data*, pp. 557-564.

Benet, J. (2014) IPFS - content addressed, versioned, P2P file system. *arXiv preprint arXiv:1407.3561*.

Groth, J. (2016) On the size of pairing-based non-interactive arguments. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 305-326.

Vukolic, M. (2015) The quest for scalable blockchain fabric: proof-of-work vs. BFT replication. In: *International Workshop on Open Problems in Network Security*, pp. 112-125.

Benchoufi, M. and Ravaud, P. (2017) Blockchain technology for improving clinical research quality. *Trials*, 18(1), p. 335.

Declarations

Funding

This study was supported by the Spanish Ministry of Science and Innovation grant PID2023-152486OB-I00 (I. Costa), the Italian Ministry of University and Research (MUR) grant PRIN 2022BK8XP (E. Ivanov), and the Swedish Research Council (Vetenskapsradet) grant 2024-04168 (A. Jensen). Red-team penetration testing conducted under agreement with Rapid7 Inc. Hospital deployment partnerships with three European hospitals (identities withheld per data use agreement). The funding bodies had no role in study design, data collection, analysis, or publication decisions.

Conflict of Interest

I. Costa is a co-inventor on a pending patent application (EP24222486.8) covering the HBF

cryptographic erasure mechanism for GDPR-compliant healthcare blockchain. E. Ivanov and A. Jensen declare no competing interests.

Data Availability Statement

HBF specification, Hyperledger Fabric chaincode, smart contracts, zero-knowledge proof circuits, HL7 FHIR gateway, and deployment configurations are available at <https://github.com/WEDSU-HealthBlockchain/HBF-2024> under Apache 2.0 licence. Aggregate deployment metrics reported in this paper; individual-level hospital data not shareable under data use agreements.

Ethical Approval

Hospital deployment conducted under IRB approval at three participating hospitals (aggregate protocol WEDSU-IRB-2024-0286). All patient data processed through HBF were already in clinical use under existing data governance. Adversarial testing conducted with hospital IT department authorisation and within defined scope agreements.

Appendix A

HBF Architecture and Cryptographic Erasure Protocol

This appendix provides the HBF four-layer architecture specification, cryptographic erasure protocol for GDPR compliance, zero-knowledge proof circuits, and deployment requirements.

A.1 Architecture Layers

- 1a. Layer 1: Hyperledger Fabric 2.5 with PBFT consensus; 8-node base + scalable addition; TLS 1.3 + mutual authentication between nodes
- 1b. Layer 2: IPFS or institutional S3-compatible storage; AES-256-GCM encryption with per-record keys; SHA-256 commitments on-chain
- 2a. Layer 3: zk-SNARK Groth16 circuits (circom + snarkjs); applications: age verification, eligibility proof, data integrity proof
- 2b. Layer 4: ERC-721-derived consent tokens with FHIR-R4 consent codes; access control via chaincode; revocation via token burn

A.2 Cryptographic Erasure for GDPR

- 3a. Data encryption: per-patient master key + per-record derived keys (HKDF); master keys stored in HSM (hardware security module)
- 3b. Deletion request: patient signs deletion authorisation; consortium validates; HSM destroys master key; audit event logged on-chain
- 4a. Post-deletion: encrypted data physically remains in storage but is computationally inaccessible (AES-256 equivalent to deleted per NIST SP 800-88)
- 4b. Verification: zero-knowledge proof that key destruction occurred; patient can verify deletion without trusting consortium