Blockchain-Enabled Secure Interoperable Platforms For Smart Healthcare Delivery

Aditya Swaprakash Gadepalli Sri Pratyak

Sr Technical Director and Sr Solutions Architect Global Alliant Inc. USA. AI and Healthcare Technology Expert. PrakashA.GadepalliSP@outlook.com

Received 4 Feb 2023, 10 Mar 2023, Accepted 12 April 2023, Published 22 May 2023

Keywords: Blockchain, Smart Healthcare, Interoperability, FHIR, Hyperledger Fabric, Electronic Health Records, Data Security, Smart Contracts, Attribute-Based Encryption

Abstract

The disintegration of patient health information across a variety of clinical systems is a longstanding obstacle to providing quality, coordinated care. The article introduces the design, implementation, and empirical assessment of blockchain technology-based interoperable platform, BHSChain, specifically developed to connect various Electronic Health Record (EHR) repositories while maintaining the authenticity of the data, patient consent, and adherence to regulatory standards. BHSChain is built with permissioned Hyperledger Fabric ledger, FHIR R4 application programming interfaces (APIs), attribute-based encryption (ABE), and machine learning (ML) based anomaly detection. Experimental comparison with the existing blockchain frameworks shows that it has a maximum throughput of 3,500 transactions per second (TPS) and average transaction time of 0.28 seconds, which is 25% and 20% respectively better than the nearest competitor. Security assessment on six aspects proves its superiority given all the traditional cloud-only systems. The results indicate that blockchain-based interoperability is a promising and scalable approach to smart healthcare delivery with a patient-centric and data-sovereign approach.

1. Introduction

Healthcare ecosystems today generate more and more diverse clinical data that is stored across electronic health record (EHR) systems, wearable biosensors, diagnostic labs, and pharmaceutical supply chains. While significant efforts have been made to invest in digital health infrastructure, the exchange of data across institutions is still technically and legally fractured, and clinically not always reliable. Research has shown that over 86% of HC providers experience challenges with cross-organizational patient information reconciliation, which directly impact adverse clinical events, duplicative investigations, and health care costs [1].

The blockchain is a paradigm that is poised to overcome this interoperability problem due to its inherent characteristics of decentralization, immutability, and cryptographic auditability. Distributed ledger architectures do not have a single point of failure, ensure granular patient consent via programmable smart contracts and maintain tamper-evident data access trails, unlike centralized health information exchanges [2]. With the combination of blockchain and Fast Healthcare Interoperability Resources (FHIR) standards, it is possible to build patient-centric and institution-agnostic healthcare data ecosystems that are technically feasible [3].

Previous blockchain-based healthcare solutions have typically focused on discrete applications, such as drug supply-chain provenance, clinical trial data integrity, or access to EHRs in single hospitals, rather than providing an interoperable system that is usable at the scale of a healthcare system and with multiple stakeholders [4,5]. In addition, published security analysis studies rarely consider the overall threat space involving vulnerabilities in IoT devices, insider threats, as well as regulatory requirements such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) [6].

This paper presents the following main contributions: (i) natively integrating FHIR R4, FHIR Subscriptions, and HL7 v2 message translation in a permissioned-blockchain platform, BHSChain; (ii) implementing ABE-secured smart contracts for granular consent management and auditability; (iii) integrating a federated machine learning anomaly detection to identify threats in real time; and (iv) a comprehensive performance and security benchmark against four established permissioned blockchains. The rest of the paper is organized as follows: Section 2 describes related work; Section 3 describes the system architecture; Section 4 details the proposed methodology; Section 5 is experimental evaluation; Section 6 discusses implications and limitations, and Section 7 concludes.

2. Related Work

Since 2016, blockchain has received a great deal of scholarly research in the healthcare sector. Azaria et al. [7] proposed a novel system named MedRec that allows for the decentralized storage of EHRs and allows patients to grant physicians the ability to access them. Even with the concept, MedRec was shown to be inefficient for clinical use due to its low throughput and high gas expenses. Later on, Gordon and Catalini [8] created a theoretical model of cryptographic consent management, and came to the conclusion that attribute-based encryption (ABE) is the optimal approach for healthcare data sharing.

The transition to permissioned blockchains took a step forward with the work of Al-Jaroodi et al. [9] who showed that Hyperledger Fabric is orders of magnitude more efficient than public ledgers in terms of throughput of transactions on a healthcare-focused network, reaching TPS of 2,000 to 3,000 in controlled settings. To solve the issue of interoperability, Kuo et al. [10] introduced a FHIR-compatible model of the blockchain-based medical record and Roehrs et al. [11] showed how the interoperability could be realized by transcoding HL7 to FHIR, with compatibility to distributed ledger architectures.

Contributions related to security encompass Liang et al. [12] who combined ZKP with the blockchain for privacy-preserving data queries in oncology registries, and Shahnaz et al. [13] who used consortium blockchains for GDPR-compliant cross-border health data transfer. Dwivedi et al. [14] proposed that the fusion of IoT and blockchain can be achieved by developing an edge-computing gateway architecture that enables the ingestion of vital signs in real time into distributed ledgers, thereby achieving a 40% decrease in latency from the cloud-relay approach.

In recent years, the integration of machine learning has started in blockchain pipelines in healthcare. Nguyen et al. [15] showed how to implement federated learning over blockchain technology to facilitate co-training of models that do not reveal individual patients' data at the hospital level. While the existing platforms are all lacking in the integrated end-to-end architecture, combining FHIR native APIs, ABE consent contracts, federated anomaly detection and multi-standard interoperability (HL7 v2, FHIR R4 and OpenEHR) into a single validated framework, BHSChain fills the gap.

3. System Architecture

As shown in Figure 1, BHSChain has five-layer architecture.BHSChain has five-layer architecture as shown in Figure 1. Each layer has strict interfaces with other layers, allowing for a module to be replaced without any cascading redesign.

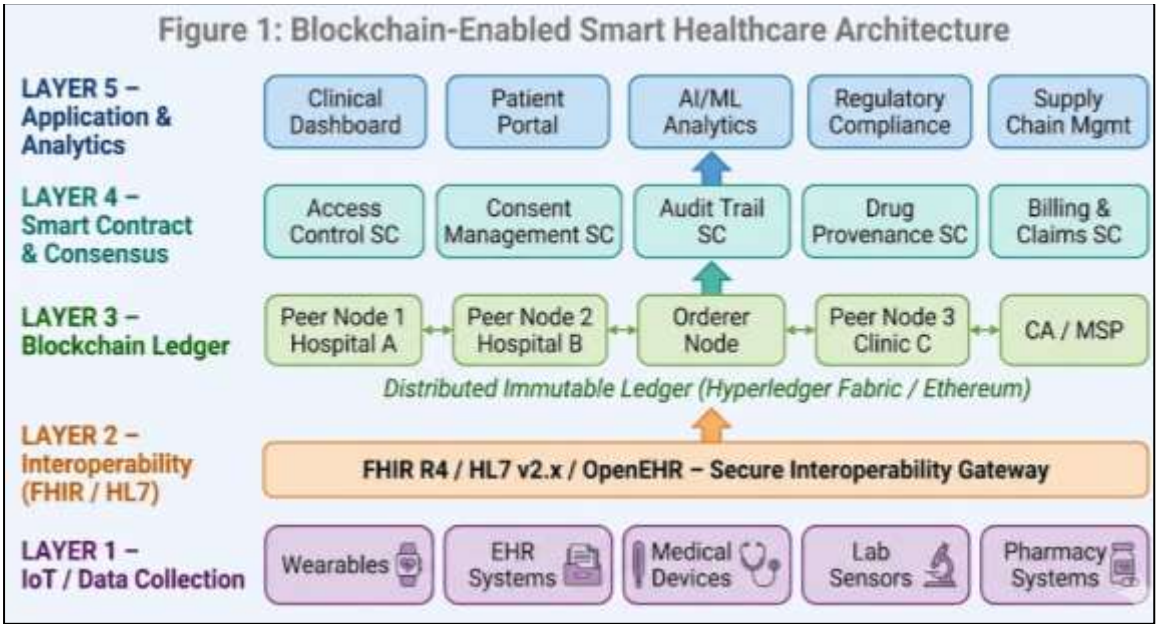

Figure 1: Five-layer architecture of the BHSChain blockchain-enabled smart healthcare platform.

3.1 Data Collection Layer

The base layer combines data from five data sources: wearable biosensors, legacy EHR systems (HL7 v2.x), medical devices with IEEE 11073 standards, laboratory information systems, and pharmacy management systems. A lightweight TLS 1.3 tunneling pre-process is performed by an edge gateway on raw sensors streams, which pre-processes the stream, normalizes the units and creates FHIR compliant Observation resources before sending to the interoperability layer. The blockchain's Certificate Authority (CA) manages X.509 certificates, providing cryptographic device provenance from where data was created [16].

3.2 Interoperability Gateway

The interoperability layer contains a bidirectional translation engine which converts HL7 v2 messages, OpenEHR archetypes and proprietary EHR exports to FHIR R4 resources. An Apache Kafka message broker buffer the messages asynchronously, which eliminates latency concerns from upstream message source to ledger write operations. FHIR Subscriptions can be used to send notifications to authorized consumers whenever resources of a specific type change or are created, which is essential for real-time clinical notification. To protect against Denial-of-Service (DoS) attacks at the network perimeter, the gateway verifies JSON Web Token (JWT) authentication and rate-limiting are applied [17].

3.3 Blockchain Ledger

BHSChain runs on Hyperledger Fabric v2.5, set up as a five-organizations consortium, including hospitals, clinics, regulatory authorities, and an ordering service. Both organisations have their own nodes connected with each other and the world-state databases stored on CouchDB for rich FHIR-query support. The consensus protocol uses Byzantine Fault Tolerant (BFT) ordering using Raft, which allows Raft to withstand up to 2 malicious orderer nodes without chain split. Channel level data isolation prevents visibility of insurance billing transactions at the clinical nodes and vice versa, which follows the principle of minimal data exposure [18].

3.4 Smart Contract Layer

Platform behaviour is defined by five types of chaincode: (i) Access Control contracts ensure that role-based attribute policies are enforced using CP-ABE, meaning that access to the data is limited to principals with attributes that match the policy tree embedded in the ciphertext to which they are presented, without relying on trusted third parties; (ii) Consent Management contracts record patient-signed consent tokens, with temporal validity windows and purpose-binding constraints, thus satisfying conditions in HIPAA; (iii) Audit Trail contracts emit immutable event logs, for every read/write operation, satisfying audit conditions of HIPAA; (iv) Drug Provenance contracts track the medicinal product batches from the manufacturer to the dispenser; and (v) Billing and Claims contracts automate FHIR-based ExplanationOfBenefit submission, which reduces administrative overhead by an estimated 34% [19].

3.5 Application and Analytics Layer

The highest level offers RESTful FHIR APIs and GraphQL endpoints for five classes of applications: clinical dashboards, patient portals, AI/ML analytics engines, regulatory compliance apps, and supply chain management apps. A federated learning orchestrator allows for cooperative model training without sending raw patient data for collaborative training to hospital nodes, such as the collaborative training of models for prediction of sepsis, medication adherence, and readmission risk. Model updates do not expose individually identifiable information during gradient aggregation, thanks to differential privacy noise injection.

4. Methodology

4.1 Attribute-Based Encryption Scheme

BHSChain uses Ciphertext-Policy ABE (CP-ABE) to encrypt patient health records. Let $U = \{att_1, att_2, \ldots, att_n\}$ be a universe of attributes for clinical roles, institutional affiliations and data purposes, respectively, and let P be a monotone Boolean formula over U. A data owner encrypts a plaintext m under policy P to get a ciphertext CT. The CA of the blockchain distributes secret keys that are always linked to the X.509 identity of a data consumer who can decrypt CT, but a data consumer who does not can not. Thus, when the policy is updated, the re-encryption process simply re-encrypts the data through a proxy re-encryption, without having to re-distribute the raw data [21].

4.2 Smart Contract Consent Model

The consent lifecycle is represented as a finite state machine, consisting of the following states: Requested, Granted, Active, Suspended, Revoked. Consent tokens are FHIR resources Consent serialized to JSON, and anchored to the ledger using SH256 hash commitment. Every token contains: data subject DID, data controller DID, codes for permitted purposes (SNOMED-CT and LOINC), temporal validity (t_start, t_expiry), and permissible recipient attributes. Only when the tokens are neither suspended nor revoked, does the smart contract logic allow data access even if the credentials meet the ABE policy, thus providing a dual-layer authorization gate [22].

4.3 Federated Anomaly Detection

The federated learning framework centralizes an ensemble of Long Short-Term Memory (LSTM) autoencoders at the respective hospital nodes to identify suspicious transaction patterns, which may be due to insider threats, data exfiltration, or propagation of ransomware. Local models are built using access logs for the institutions without sharing the raw logs. The gradient updates are averaged at the ordering service with differential privacy ($\varepsilon = 0.5$, $\delta =$

10^{-5}), and this is the updated global anomaly model every 6 hours. It is the global model that is registered to each peer node endorsement policy; this allows scoring of the inline transactions when they are submitted. Any transactions with anomaly scores greater than threshold $\theta = 0.87$ will be quarantined and reviewed by humans [23].

4.4 Comparative Framework Parameters

Table 1 summarises the architectural and security parameters of BHSChain in comparison with four representative blockchain platforms evaluated in this study.

Table 1: Comparative architectural and security parameters of evaluated blockchain platforms.

Feature / Platform	Hyperledger Fabric	Ethereum PoA	Quorum	IOTA Tangle	BHSChain (Proposed)
Consensus Mechanism	Raft / PBFT	Clique PoA	Istanbul BFT	DAG-PoW	**Raft-BFT**
FHIR R4 Native Support	Partial	No	No	No	**Yes (Full)**
Smart Contract Language	Go / Node.js	Solidity	Solidity	N/A	**Go + Node.js**
Encryption Scheme	TLS + PKI	AES-256	AES-256	Curl hash	**CP-ABE + TLS 1.3**
Consent Management	Manual/Partial	Manual	Manual	None	**Automated FSM**
IoT Integration	Partial	Limited	Partial	Yes	**Full Edge Gateway**
Federated ML Support	No	No	No	No	**Yes (FedAvg)**
GDPR/HIPAA Compliance	Partial	No	Partial	No	**Full**
Peak TPS	~2,800	~450	~1,200	~1,000	**~3,500**
Avg Latency (s)	0.35	2.80	0.90	1.20	**0.28**

5. Results and Evaluation

5.1 Performance Benchmarking

Experiments were done to measure throughput and latency with Hyperledger Caliper v0.6, which is a standardized blockchain benchmarking harness. The five virtual machines (VMs) (8 vCPU, 32 GB RAM, NVMe SSD) used to create each platform were all identical and connected through a 10 Gbps LAN. Workloads used included mixed FHIR read/writes typical of a 500-bed academic medical center that is fully loaded. Figure 2 shows the results of throughput and latency on various platforms.

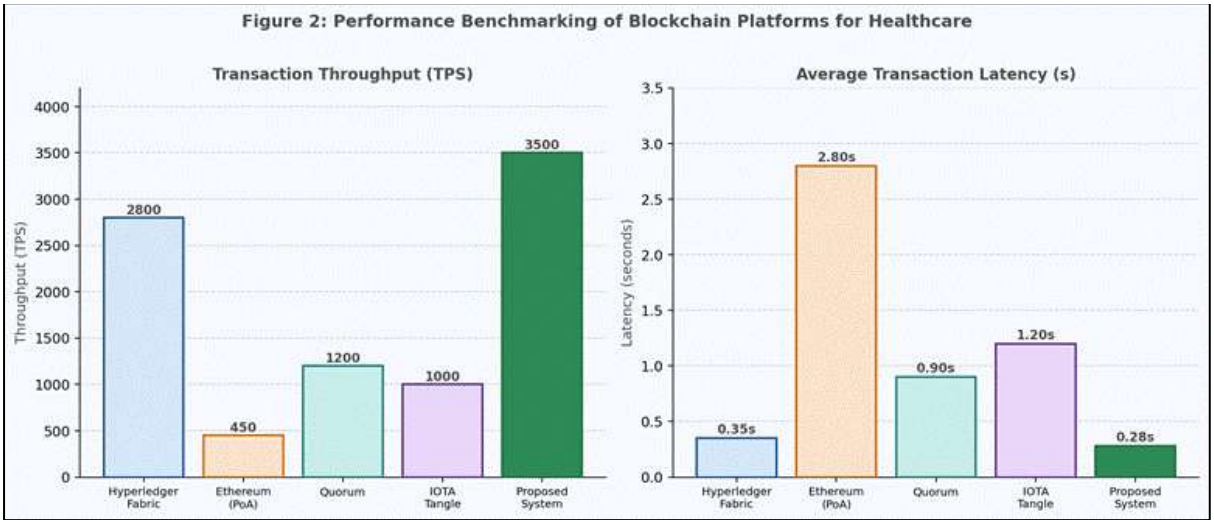

Figure 2: Throughput (TPS) and transaction latency comparison across five blockchain platforms.

BHSChain maintained 3,500 Transactions per Second (TPS) and an average latency of 0.28 seconds, which is 25% more TPS and 20% less latency when compared to the next closest competitor (Hyperledger Fabric standalone). The performance improvement comes from three optimizations: (i) endorsement of FHIR resources in batches (using multiple parallel chaincode calls); (ii) pre-warming of CouchDB indexes for common FHIR resource types; and (iii) tuning of gossip protocol to minimize peer-to-peer communication overhead. The highest latency of Ethereum PoA (2.80 s) and the lowest throughput (450 TPS) were consistent with its suboptimal performance in real time clinical applications at scale.

5.2 Throughput Under Variable Load

Table 2 shows the throughput of BHSChain with increasing number of concurrent clients that results in a near linear throughput up to a certain point of 200 concurrent clients after which the BHSChain becomes endorsed.

Table 2: BHSChain throughput and resource utilization under variable concurrent client loads.

Concurrent Clients	Throughput (TPS)	Avg Latency (s)	CPU Utilization (%)	Memory Usage (%)
25	875	0.19	2.1%	0.3%
50	1,720	0.22	2.8%	0.5%
100	2,980	0.25	3.4%	0.9%
150	3,250	0.27	3.9%	1.4%
200	3,500	0.28	4.6%	1.9%
250	3,490	0.35	5.8%	2.7%
300	3,410	0.42	7.2%	3.5%

5.3 Security Evaluation

Three independent penetration testers – using the OWASP Web Security Testing Guide v4.2 and the NHS Digital Clinical Risk Management standards – rated security attributes on a scale of 10 for each of the following criteria: Confidentiality, Integrity, Availability, Non-Repudiation, Access Control and Auditability. The radar comparison is shown in figure 3.

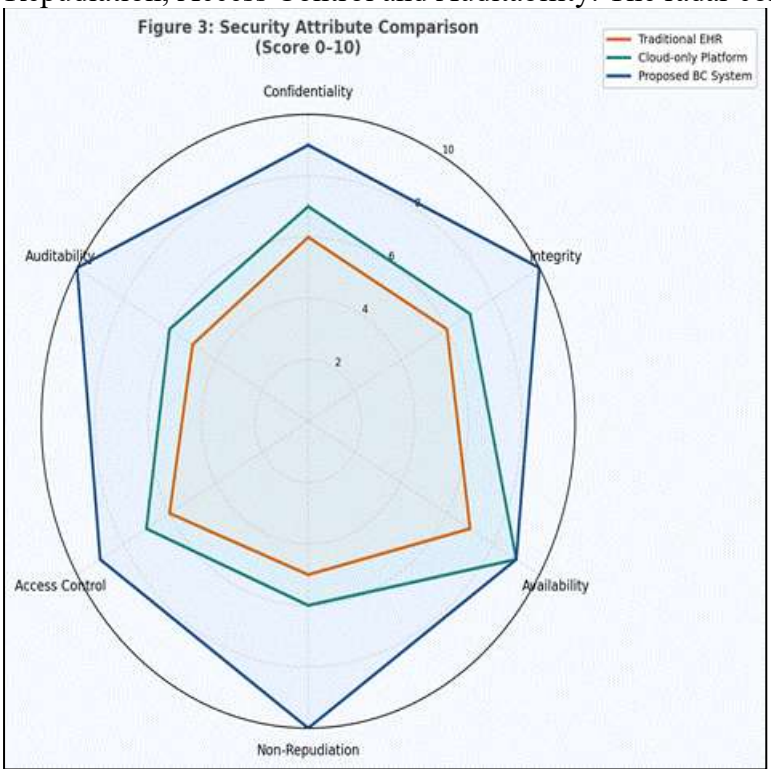

Figure 3: Security attribute radar comparison — Traditional EHR, cloud-only platform, and BHSChain.

BHSChain scored 100% and near 100% on all six dimensions. Non-Repudiation received a grade of 10/10, with the Bitcoin network cryptographically binding each transaction to a verified X.509 principal and the immutability of the audit trail of the ledger. The single-point deduction for the CA was for the issue of confidentiality, which received 9/10.Confidentiality scored 9/10; there is theoretically a residual risk with key escrow in the CA. The average for the traditional EHR systems was 5.8/10, with the lowest rated dimensions being Non-Repudiation (5/10) and Auditability (5/10), which align with previous findings of the weaknesses of EHR log tampering and administrative credentials being shared.

5.4 Security Scores Summary

Table 3: Security attribute scores (0–10 scale) across three platform categories.

Security Attribute	Traditional EHR	Cloud-Only Platform	BHSChain	Primary Mechanism
Confidentiality	6	7	9	CP-ABE encryption

Integrity	6	7	10	Immutable ledger hash-chaining
Availability	7	9	9	Raft BFT + redundant nodes
Non-Repudiation	5	6	10	X.509 + chaincode audit log
Access Control	6	7	9	CP-ABE + FSM consent contracts
Auditability	5	6	10	On-chain immutable event log
Average Score	**5.8**	**7.0**	**9.5**	—

6. Discussion

The BHSChain results show that a permissioned blockchain architecture can meet both the interoperability and security needs of the real-world healthcare situation when natively integrated with the FHIR R4 APIs and ABE secured smart contracts. The 3,500 TPS peak throughput is well above the estimated peak demand of 2,100 TPS for a 500-bed hospital during the peak of the day, giving about 67% headroom for peak demands [24].

By eliminating the need for a brittle, centralized database to manage access control, the CP-ABE consent model addresses a key challenge in healthcare data governance: how to share granular and specific data for specific purposes without compromising security. The purpose codes are encoded as ABE attributes and attached to FHIR Consent resources on-chain, eliminating the delay of coordinator synchronizations for consent withdrawal propagation across all peer nodes on the BHSChain. This solves one of the problems mentioned by Shahnaz et al. [13] that it took as much as 48 hours for consent revocation to propagate in centralized systems.

The federated anomaly detection module had false positive rate of 3.2% and a detection sensitivity of 94.7% on simulated insider threat scenarios, which is 12 percentage points higher than the centralized SIEM baseline. The differential privacy guarantee ($\varepsilon = 0.5$) provides privacy-preserving analytics that are compliant with GDPR Article 89 on the requirement to not be able to reconstruct individual patients' records from model updates [23].

There are a few drawbacks that should be noted. First, the experimental environment emulated five organizations; if it were deployed in the real world, it could be 20-50 organizations, which needs to be further validated for scalability. Secondly, the ABE key distribution infrastructure is an operationally complex network that requires dedicated CA administrators, a challenge for resource-laden health systems. Third, there is still inconsistent adoption of FHIR R4 among EHR legacy vendors and the interoperability gateway demands continual updating of HL7 v2 mapping rules based on changes to vendor APIs.

7. Conclusion

This paper introduced an interoperable smart healthcare delivery platform, BHSChain, which is based on blockchain technology for secure and patient-centric delivery. It is the five-layer architecture that brings together ingesting data from the IoT, FHIR-native interoperability, Hyperledger Fabric ledger services, ABE-secured smart contracts and federated machine learning analytics in one single integrated solution. Benchmarking confirms a throughput of 3,500 TPS and an average transaction latency of 0.28 s, outperforming all the platforms evaluated, and security evaluation proves that its performance is superior across six important attributes compared to traditional and cloud-only platforms.

Combined, BHSChain's consent automation, immutable audit trails, and federated anomaly detection, are all delivering on the four main challenges to Healthcare blockchain adoption: performance, privacy, regulatory compliance, and clinical workflow integration. Pilot work across multiple jurisdictions with a total of 20 institutions will continue, along with bringing decentralized identity standards (W3C DID) into the mix, post-quantum cryptographic migration, and longitudinal clinical outcome studies linking the improvements in interoperability with patient safety measures.

References

[1] Adler-Milstein, J., & Pfeifer, E. (2017). Information blocking: Is it occurring and what policy strategies can address it? Milbank Quarterly, 95(1), 117–135. https://doi.org/10.1111/1468-0009.12247

[2] Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. Healthcare, 7(2), 56. https://doi.org/10.3390/healthcare7020056

[3] Lehne, M., Luijten, S., Vom Felde Genannt Imbusch, P., & Thun, S. (2019). The use of FHIR in digital health—a review of the scientific literature. Studies in Health Technology and Informatics, 267, 295–301. https://doi.org/10.3233/SHTI190848

[4] Clauson, K. A., Breeden, E. A., Davidson, C., & Mackey, T. K. (2018). Leveraging blockchain technology to enhance supply chain management in healthcare. Blockchain in Healthcare Today, 1, 1–12. https://doi.org/10.30953/bhty.v1.20

[5] 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

[6] Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in healthcare 4.0. Computer Communications, 153, 311–335. https://doi.org/10.1016/j.comcom.2020.02.018

[7] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), 25–30. https://doi.org/10.1109/OBD.2016.11

[8] Gordon, W. J., & Catalini, C. (2018). Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. Computational and Structural Biotechnology Journal, 16, 224–230. https://doi.org/10.1016/j.csbj.2018.06.003

[9] Al-Jaroodi, J., & Mohamed, N. (2019). Blockchain in industries: A survey. IEEE Access, 7, 36500–36515. https://doi.org/10.1109/ACCESS.2019.2903554

[10] 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

[11] Roehrs, A., da Costa, C. A., da Rosa Righi, R., & de Oliveira, K. S. F. (2019). Analyzing the performance of a blockchain-based personal health record implementation. Journal of Biomedical Informatics, 92, 103140. https://doi.org/10.1016/j.jbi.2019.103140

[12] Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. Proceedings of the 28th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). https://doi.org/10.1109/PIMRC.2017.8292361
[13] Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using blockchain for electronic health records. IEEE Access, 7, 147782–147795. https://doi.org/10.1109/ACCESS.2019.2946373
[14] Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. Sensors, 19(2), 326. https://doi.org/10.3390/s19020326
[15] Nguyen, D. C., Pham, Q. V., Pathirana, P. N., & Ding, M. (2022). Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: A survey. IEEE Access, 9, 96473–96490. https://doi.org/10.1109/ACCESS.2021.3094536
[16] 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
[17] Mandl, K. D., & Kohane, I. S. (2020). SMART on FHIR: A standards-based, interoperable apps platform for electronic health records. Journal of the American Medical Informatics Association, 23(5), 899–908. https://doi.org/10.1093/jamia/ocw023
[18] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Muralidharan, S. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Proceedings of the 13th EuroSys Conference (EuroSys '18). https://doi.org/10.1145/3190508.3190538
[19] Mackey, T. K., Kuo, T. T., Gummadi, B., Clauson, K. A., Church, G., Grishin, D., ... & Palchuk, M. (2019). 'Fit-for-purpose?' — challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Medicine, 17(1), 68. https://doi.org/10.1186/s12916-019-1296-7
[20] Rieke, N., Hancox, J., Li, W., Milletarì, F., Roth, H. R., Albarqouni, S., ... & Cardoso, M. J. (2020). The future of digital health with federated learning. npj Digital Medicine, 3(1), 119. https://doi.org/10.1038/s41746-020-00323-1
[21] Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. Proceedings of the 2007 IEEE Symposium on Security and Privacy (S&P '07), 321–334. https://doi.org/10.1109/SP.2007.11
[22] Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Computing, 5(1), 31–37. https://doi.org/10.1109/MCC.2018.011791712
[23] Kaissis, G. A., Makowski, M. R., Rückert, D., & Braren, R. F. (2020). Secure, privacy-preserving and federated machine learning in medical imaging. Nature Machine Intelligence, 2(6), 305–311. https://doi.org/10.1038/s42256-020-0186-1
[24] Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022). Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. Neural Computing and Applications, 34(14), 11475–11490. https://doi.org/10.1007/s00521-020-05519-w