Proceedings of CONF-CDS 2026 Symposium: Data-Centric AI Security: Securing Models, Learning Agents, and Autonomous Systems
DOI: 10.54254/2755-2721/2026.CH34597

Patient-Centric Secure Medical Record Sharing on Ethereum: Topic Analysis and Proof-of-Concept

Zhe Zhang

School of Finance, Southwestern University of Finance and Economics, Chengdu, China
13981852683@163.com

Abstract. This paper investigates Ethereum-based smart contracts as a decentralized cybersecurity governance layer for Electronic Medical Records (EMRs). It addresses challenge of fragmented healthcare data silos and strict compliance requirements for electronic protected health information (ePHI), such as HIPAA and GDPR by analyzing how blockchain technology enables explicit, patient-centric access control. Current legacy systems often centralize authorization, creating vulnerablilities. Through topic analysis and a Solidity-based Proof of Concept (PoC), the study demonstrates a hybrid architecture that uses on-chain execution for permission management while storing sensitive clinical data off-chain. The PoC shows how immutable ledger entries enforce least-privilege principles, block unauthorized queries, and provide tamper-evident auditability. The architecture's trade-offs between enhanced accountability, patient sovereignty, and practical limitations in scalability, governance, and costs are assessed. It concludes that while blockchain offers a robust trust layer, integration with off-chain interoperability standards remains essential for clinical adoption.

Keywords: Electronic Medical Records, Ethereum Smart Contracts, Patient-Centric Access Control, Blockchain Healthcare, Hybrid Architecture

1. Introduction

Electronic medical records (EMRs) promise longitudinal, portable clinical histories, yet real-world exchange remains constrained by fragmented governance and cybersecurity risk. In practice, patient data are distributed across institutions and vendors, leading to "siloed" information flows, repeated intake, and delays in cross-provider coordination. Meanwhile, regulated entities must implement technical safeguards—including access control, audit controls, integrity mechanisms, authentication, and transmission security—for electronic protected health information (ePHI) [1]. In the EU context, data protection and accountability requirements further shape how health data can be processed and shared [2]. These requirements imply that any proposed sharing architecture should make authorization explicit, minimize unnecessary disclosure, and produce defensible audit trails.

This paper analyzes whether blockchain-based permission management can serve as a cybersecurity- oriented governance layer for EMR sharing. Building on the smart contract concept of proactively enforced rules, and on widely studied blockchain properties, such as tamper-evident logging and decentralized consensus, this paper focuses on a narrow but high-value control point:

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/2026.CH34597

who is authorized to retrieve an EMR reference [3-6]. Prior healthcare blockchain research commonly converges on a hybrid architecture in which clinical payloads remain off-chain while the ledger stores pointers/hashes, access policies, and access-related events [7-10]. This division is largely motivated by privacy, compliance, and storage constraints. This paper frames the problem as an access-control and auditability problem under a practical threat model: unauthorized external accounts attempting to query or obtain record references, insider misuse (over-broad access), and disputes over whether an authorization existed at a given time. The research question is: Can a minimal Ethereum smart contract enforce patient-centric authorization for accessing EMR references, and produce evidence of com- pliant access decisions, while acknowledging the limits of on-chain computation and storage? We answer this question via topic analysis and a demonstrable proof-of-concept (PoC) implemented in Solidity.

2. Related work

Blockchain has been studied in health informatics primarily as a coordination mechanism—not as a repository for raw clinical data. Early proposals, such as the Healthcare Data Gateway, advocate patient ownership and control of health data while emphasizing privacy risk control and auditable computation [11]. A widely cited JAMIA review summarizes comparative advantages (e.g., immutable audit trails and provenance) and highlights key pitfalls, such as transparency/confidentiality tension and scalability constraints [10]. Subsequent systematic reviews identify EMR/PHR sharing as a dominant application area, yet note persistent barriers in performance, governance, and deployment cost [12, 13]. Across concrete system designs, a recurring pattern is to keep clinical payloads off-chain and use blockchain to manage permissions and audit logs. MedRec, an influential early prototype, uses blockchain to manage medical data access rights and maintain an immutable log of access events [7]. FHIRChain connects blockchain-based authorization with clinical data exchange workflows aligned with HL7 FHIR interoperability standards [8, 14, 15]. More recent patient-centric systems such as ACTION-EHR emphasize fine-grained, patient-specified access policies for secure cross-hospital sharing [9]. Consortium or permissioned approaches (e.g., HealthChain, Hyperledger Fabric) explore governance models and higher throughput under restricted membership [16, 17].

From a cybersecurity perspective, these works support a core principle: blockchains can provide consistent, cross-organizational authorization state and tamper-evident auditability but they do not replace conventional security controls (e.g., identity proofing, key management, secure off-chain storage, and revocation workflows). Moreover, smart contracts introduce a software attack surface; prior Ethereum analyses document common vulnerability classes and underscore the difficulty of correcting bugs after deployment [17]. This paper therefore adopts a minimal PoC scope: no on-chain clinical data storage, and strict focus on correct authorization enforcement and denial behavior.

Despite the proliferation of conceptual frameworks and complex consortium models, a critical research gap remains in isolating the core cybersecurity mechanics of on-chain access control. Many implementations conflate permission logic with heavy off-chain routing or proprietary identity layers, obscuring the smart contracts' fundamental deterministic enforcement capability. Targeted studies evaluating the bare-minimum baseline for secure, patient-controlled authorization are scarce. To bridge this gap, this paper shifts focus from building comprehensive clinical platforms to validating a fundamental cybersecurity primitive: demonstrating specifically how a minimal Ethereum smart contract can mathematically enforce patient-centric access boundaries (allow/deny)

DOI: 10.54254/2755-2721/2026.CH34597

and produce a tamper-evident audit trail, thereby providing a transparent, verifiable foundation for EMR governance.

3. System design

3.1. System overview

The proposed system is a patient-centric access-control and audit layer for EMR sharing. It does not replace hospital information systems nor store clinical data on-chain; instead, it enforces explicit, verifiable and tamper-evident authorization rules for accessing EMR references. This aligns with the dominant healthcare blockchain pattern: blockchain handles governance, permissions, and auditability, while clinical payloads reside in secure, compliant off-chain repositories [7-12]. The architecture is hybrid. The blockchain layer stores only minimal governance data: a patient-owned EMR reference or hash and its associated authorization state—i.e., which external address is permitted to retrieve it. The off-chain layer hosts the actual EMR payload, such as diagnostic reports, images, physician notes, or HL7 RHIR-structured records [14, 15]. Figure 1 illustrates this division of responsibilities between on-chain logic and off-chain data.

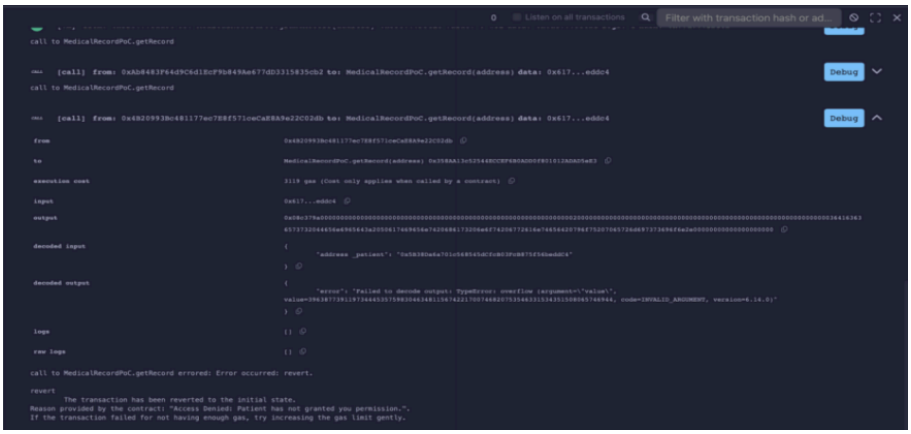

Figure 1. System architecture of the proposed patient-centric EMR sharing model

Three roles define the system: (1) The patient: the data owner and sole authority to grant or revoke access; (2) The healthcare provider: the requesting party, authorized to retrieve the EMR reference only upon explicit patient consent; (3) The blockchain network: the decentralized environment where smart contracts enforce access rules deterministically. This role allocation reflects the patient-centric governance model established in MedRec, FHIRChain, and ACTION-EHR [7-9].

3.2. Access control model

The access-control model adopted in this paper is a patient-centric discretionary authorization model implemented at the smart contract layer. The core principle is that the patient, as the data subject and controller of the record reference in this PoC, determines whether a doctor's address may access the corresponding EMR reference. This scope is intentionally narrower than full role-based or attribute-based access control systems used in enterprise healthcare settings; however, it suffices to demonstrate the core governance logic of patient-authorized sharing.

DOI: 10.54254/2755-2721/2026.CH34597

Formally, the model comprises three elements: subjects, objects, and permissions. A subject is an externally owned blockchain address, typically representing a patient or a doctor. An object is the patient-associated EMR reference stored in the contract. A permission is a binary authorization relation indicating whether a specific doctor's address is allowed to retrieve a specific patient's EMR reference. In implementation, this relation is represented by a nested mapping that associates each patient address with a set of doctor addresses and Boolean access values.

The model supports two main security properties: (1) explicit authorization: doctors cannot access a patient's EMR reference unless the patient has actively granted permission before-hand; (2) default denial: any access request is rejected unless a positive authorization state exists. This default-deny logic is important from a cybersecurity perspective: it reduces ambiguity in enforcement and provides a clear boundary against unauthorized external access. Practically, the contract implements least privilege by granting only the minimal necessary access to designated addresses and by withdrawing broader read rights from unspecified participants.

This model also enhances auditability. Because permissions are created via on-chain transactions and emit corresponding events, the contract produces a verifiable audit trail showing when and by which blockchain account authorization was granted. Such a trail supports later review, accountability, and dispute resolution—central requirements in regulated health information environments [1, 10]. At the same time, the model is deliberately simplified and does not purport to satisfy all real-world access-governance needs. In particular, it omits revocation, time-limited permissions, delegated consent, emergency "break- glass" overrides, and linkage to real-world identity proofing. These omissions are acceptable in a PoC, whose goal is to validate the core access-decision mechanism not to replicate the full complexity of production-grade clinical governance.

3.3. Smart contract design

The smart contract is a minimal Ethereum-based module for storing EMR references and enforcing patient-controlled access. Designed as a deterministic rule engine, it processes transactions to update state and evaluates read requests against predefined conditions [3, 5, 6]. Its compact design focuses attention on the essential question: can explicit, on-chain patient authorization be reliably enforced?

It supports three operations: Record registration: a patient stores an EMR reference or hash associated with their address; actual clinical data remains off-chain; Access granting: the patient authorizes a specific doctor's address; Record retrieval: a doctor requests the EMR reference; the contract checks authorization first and reverts with "access denied" if unauthorized.

Two internal mappings implement this logic: One maps patient addresses to their EMR references. The other maps each patient address to a set of authorized doctor addresses (Boolean permissions). This separation isolates data reference management from permission management—ensuring records are never globally readable by default, and all access is gated through authorization. The contract emits events on record updates and permission grants. These provide a amper-evident, auditable log of key actions (e.g.,hash registeration, consent grant), enabling accountability and post hoc verification—key advantages in blockchain-based healthcare systems [7, 10].

Three deliberate design decisions underpin the PoC: (1) Storing only hashes, not raw medical data to avoid privacy, regulatory, and scalability problems on public blockchains [1, 2, 11]. (2) Using simple Boolean permissions rather than complex policy languages, reducing overhead and improving conceptual verifiability. (3) Excluding real-world identity binding (e.g., linking addresses to licensed physicians), a critical deployment concern but outside this PoC's scope. Here, we assume

DOI: 10.54254/2755-2721/2026.CH34597

valid addresses are known and test whether the contract can consistently and transparently enforce patient-defined rules. As shown in Figure 1, the contract serves as the on-chain policy enforcement point bridging patient authorization and doctor access.

3.4. Proof of concept demonstration

Implemented in Solidity and tested in Remix (JavaScript VM), this PoC validates the core access-control logic: patient-owned record registration, explicit access granting, authorized retrieval, and unauthorized denial. It is not a full healthcare system stimulation but a design validation showing that the proposed model can be concretely enforced via deterministic smart contract execution on Ethereum.

The workflow follows Figure 1: First, a patient registers an EMR reference on chain; Second, the patient grants access to a specific doctor's address. Third, an authorized doctor retrieves the reference successfully. Finally, an unauthorized account calling the same function triggers a revert with "Access Denied: Patient has not granted your permission." This confirm enforcement, not just recording of patient-defined permissions at the blockchain layer.

The unauthorized-access test (Figure 1) is the most security-relevant result. It demonstrates strict default-deny behavior: absence of permission yields no partial disclosure or ambiguity, only a clean, deterministic rejection. This validates three key properties underpinning our technical claim: authorization is explicit, enforcement is deterministic, and denials occur at the contract level. These establish a clear logical boundary between permitted and non-permitted access attempts.

At the same time, the PoC remains intentionally limited in scope. It omits revocation, time-limited permissions, emergency overrides, off-chain encryption, and identity federation with hospitals and regulators. It also does not benchmark throughput, latency, or transaction cost under loads. These limitations are methodological, not deficiencies. The goal is to verify feasibility of the core authorization logic under a simplified threat model, providing a minimal yet concrete foundation for discussing benefits, limitations, and future work.

4. Security analysis

This section evaluates the system's cybersecurity properties, focusing on what the PoC actually delivers: on-chain access-control enforcement, data integrity and auditability of reference, and privacy-aware separation of on-chain logic from off-chain data. It also clarifies key design limitations and underlying security assumptions

4.1. Access control enforcement

The core objective is to enforce patient-centric access control over EMR references, implemented directly in the smart contract. A doctor's address must be explicitly authorized by the patient before retrieval is allowed. Absent that authorization, the contract reverts with "Access Denied," enforcing a strict default-deny policy, a fundamental security principle.

This mechanism has two advantages: First, the enforcement logic is deterministic. Decisions are made by immutable contract code under Ethereum consensus not by discretionary human judgment, ensuring predictability and testability. Second, authorization is explicit and patient-directed. Unlike institution-centric models (e.g., role inheritance), access here requires direct, verifiable consent from the data subject. The unauthorized-access test validates this: calling `getRecord` with an unapproved

DOI: 10.54254/2755-2721/2026.CH34597

address triggers an immediate revert—not silent failure or partial disclosure. The contract thus acts as an active policy enforcer, not a passive permission registry.

However, enforcement strength depends on critical assumptions. Most importantly, blockchain addresses must map correctly to real-world actors. The contract cannot verify identity, licensure, or intent; if a malicious actor controls a doctor's private key or the patient authorizes the wrong address, the contract executes faithfully but insecurely. Thus, the PoC proves logical access enforcement at the blockchain layer but not full identity assurance in a clinical deployment context.

4.2. Data integrity and auditability

The contract stores only EMR references or hashes, not full records, leveraging blockchain immutability for tamper-evident anchoring. While not absolute protection against all operational risks, on-chain storage makes unauthorized alteration of confirmed state significantly harder than in centralized databases.

This supports integrity in two ways: (1) Reference anchoring: any unauthorized change to the off-chain payload creates a detectable mismatch with the on-chain hash. (2) Event-driven audit trail: the contract emits events on record registration and access grants, creating a transparent, time-stamped log of governance actions, allowing observers to verify when a patient registered a reference and when a doctor was authorized.

Such a trail meets core healthcare governance needs: it provides defensible records of who was permitted to access what, and when, enabling accountability, dispute resolution, and compliance reviews. This aligns with established use of blockchain for provenance and audit support in health data sharing.

That said, on-chain integrity does not extend to the entire EMR ecosystem. Off-chain storage, ingestion pipelined, user interfaces, and key management remain outside the contract's scope. If the off-chain repository is compromised, if the original uploaded content is false, or if a legitimate user's private key is stolen, the blockchain may preserve a faithful record of those actions without being able to prevent them. Therefore, the integrity benefit provided by the PoC should be understood as integrity of authorization state and reference anchoring, not complete end-to-end protection of all clinical data assets.

4.3. Privacy considerations

Privacy is a core concern, driving the PoC's hybrid architecture. Raw EMR content is kept off-chain; only abstract references or hashes are stored on-chain. This is essential: public blockchains expos data broadly, prohibit deletion, and incur high update costs, clashing with legal, ethical, and operational privacy requirements.

By isolating clinical payloads off-chain, the design limits exposure of ePHI. The blockchain handles only minimal governance metadata, enabling access control and auditability, while supporting privacy principles like data minimization, controlled access, and accountability. In practice, it records who is authorized and what reference belongs to which patient, sensitive medical data reside in a controlled environment where encryption, access logging, and institutional security policies apply.

Still, privacy risks persist. Metadata leakage remains possible: transaction timing, address interaction patterns, or even the mere existence of a patient-doctor link may reveal sensitive information under certain threat models. Moreover, if the on-chain reference is poorly designed, or can be linked to identifiable off-chain records, the privacy value of off-chain storage erodes. Thus,

DOI: 10.54254/2755-2721/2026.CH34597

metadata minimization and linkability reduction must be deliberate designing goals, not assumed outcomes of using hashes.

Finally, privacy depends critically on the off-chain layer. Encryption, access management, storage security, and compliant handling remain essential. The blockchain supports privacy-preserving governance, but cannot guarantee confidentiality of medical information. The proposed PoC should be interpreted as privacy-aware rather than privacy-complete.

4.4. Limitations

This PoC has five key limitations. First, authorization is simplified: it supports granting but omits revocation, time-bounded consent, delegation, multi-party approval, or emergency "break-glass" access, features essential in dynamic clinical settings. Second, it assunmes trusted identity-binding: addresses must already map to verified real-world actors (e.g., licensed physicians); the contract itself cannot validate identity or preventing misbinding. Third, smart contract security is not comprehensively addressed—production use would require rigorous code review, formal analysis, vulnerability scanning, and upgrade planning. Fourth, performance and cost are untested under realistic loads: public blockchains impose latency, throughput limits, and gas fees that may hinder scalability.

Finally, end-to-end security is out of scope, the PoC validates only on-chain enforrcement of patient-defined EMR reference access, not off-chain storage, identity systems, infrastructure, workflows, or human practices. Its contribution is a focused demonstration of blockchain-based authorization and audit support, not as a complete solution to healthcare cybersecurity.

5. Discussion

The proposed patient-centric authorization approach offers several notable advantages. By allowin patients to update the authorization state themselves, the system supports least-privilege sharing that is not coupled to any single institution's internal access-control system. This aligns with the dominant motivation identified in PHR/EHR blockchain studies, which emphasize shifting control and ownership toward end users while keeping an auditable policy trail [9, 12, 13]. Additionally, the ability to log permission grants and record updates as transactions provides tamper-evident audit and accountability, providing strong evidence for forensic review and dispute resolution. Such capabilities directly address technical safeguard expectations, such as audit controls, integrity mechanisms, and authentication in ePHI systems [1]. Prior prototypes explicitly cite immutable logging as a benefit for medical data access governance [7, 10]. Furthermore, blockchain serves as an interoperability-friendly governance layer rather than a replacement for existing standards. Solutions like FHIRChain illustrates how blockchain-based authorization can integrate with HL7 FHIR workflows, supporting cross-organization data exchange and complementing interoperability standards [8, 14, 15].

Despite these advantages, several challenges remain. Scalability and cost constraints present significant barriers, as public-chain execution incurs latency and fees that make frequent updates or large-scale workflows impractical. While permissioned or consortium blockchain designs can improve throughput under membership assumptions, this comes at the cost of reduced openness and different trust models [16, 17]. Privacy and compliance engineering remains complex, as storing clinical data on-chain is generally inappropriate, and secure off-chain storage, encryption, identity proofing, and key management remain mandatory. Regulatory obligations, such as HIPAA technical safeguards and GDPR principles, are not automatically satisfied by blockchain usage, and poor

DOI: 10.54254/2755-2721/2026.CH34597

implementation can negate purported benefits [1, 2]. Smart contract risks also pose concerns, as vulnerabilities and bugs are difficult to patch post-deployment, highlighting the need for minimal PoC implementations, careful scope control, and strong engineering discipline in production systems. Finally, real world deployments must support revocation, time-bounded permissions, delegation, and break-glass access, which are frequently discussed as gaps between prototypes and deployable systems [10, 11, 13].

6. Conclusion

This paper explores blockchain's role in patient-centric EMR sharing, focusing on cybersecurity and governance. It does not propose replacing existing healthcare systems, but asks whether blockchain can serve as a reliable, on-chain control layer for authorization and accountability in cross-organizational data sharing. To answer this, the paper combines conceptual analysis with a minimal Ethereum-based PoC.

Results confirm that blockchain can enforce explicit, patient-defined authorization over EMR references. Patients control which doctor addresses may retrieve their record reference and the smart contract enforces this deterministically, not through discretionary processes. The PoC cleanly distinguishes authorized from unauthorized access, retrieval succeeds only when permission exists; all other revert with "Access Denied." This validates its utility as a practical policy-enforcement mechanism not just theory. A second contribution is enhanced auditability without on-chain clinical data. By immutably logging record updates and consent grants, the system creates a transparent history of security-relevant actions.

Yet blockchain alone is insufficient for healthcare cybersecurity. It does not remove the need for secure off-chain storage, identity verification, encryption, interoperability standards, or broader institutional governance. Its realistic role is complementary: ensuring consistent access control and verifiable authorization.

Overall, patient-centric blockchain authorization is technically feasible and offers meaningful governance benefits. However, scaling to real-world deployment requires robust support for revocation, delegation, emergency access, identity and contract assurance, and performance evaluation. Future work should extend this functional prototype into an operationally viable security architecture for healthcare data sharing.

References

[1] eCFR. (n.d.). 45 CFR 164.312-Technical safeguards. Retrieved February 24, 2026, from https: //www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.312.
[2] European Union. (2016) Regulation (EU) 2016/679 (General Data Protection Regulation). Retrieved February 24, 2026, from https: //www.legislation.gov.uk/eur/2016/679/contents.
[3] Szabo, N. (1996) Smart contracts: Building blocks for digital markets. Retrieved from https: //www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/ LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.
[4] Nakamoto, S. (2008) Bitcoin: A peer-to-peer electronic cash system. https: //bitcoin.org/bitcoin.pdf.
[5] Buterin, V. (2014) Ethereum: A next-generation smart contract and decentralized application platform.https: //blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_ platform-vitalik-buterin.pdf.
[6] Wood, G. (2014) Ethereum: A secure decentralised generalised transaction ledger (yellow paper). https: //ethereum.github.io/yellowpaper/paper.pdf.
[7] Azaria, A., Ekblaw, A., Vieira, T., et al. (2016) MedRec: Using blockchain for medical data access and permission management. 2016 2nd International Conference on Open and Big Data (OBD), 25–30.

DOI: 10.54254/2755-2721/2026.CH34597

[8] Zhang, P., Schmidt, D. C., White, J., et al. (2018) FHIRChain: Applying blockchain to securely and scalably share clinical data. Computational and Structural Biotechnology Journal, 16: 267–278.
[9] Dubovitskaya, A., Xu, Z., Ryu, S., et al. (2020) Action-EHR: Patient-centric blockchain-based electronic health record data sharing system. Journal of Medical Internet Research, 22(8): e13598.
[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.
[11] Tandon, A., Dhir, A., Islam, A. K. M. N., et al. (2020) Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. Computers in Industry, 122: 103290.
[12] Yue, X., Wang, H., Jin, D., et al. (2016) Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 40(10): 218.
[13] Fang, H.S., et al. (2021) Blockchain personal health records: Systematic review. Journal of Medical Internet Research.
[14] HL7. (n.d.). FHIR overview. HL7 FHIR Specification. Retrieved from February 24, 2026, from https: //www.hl7.org/fhir/overview.html.
[15] Ayaz, M., Pasha, M. F., Alzahrani, M., et al. (2021) The fast health interoperability resources (FHIR) standard: Systematic literature review of implementations, applications, challenges and opportunities. JMIR Medical Informatics, 9(7): e21929. https: //doi.org/10.2196/21929
[16] Xiao, Y., Xu, B., Jiang, W., et al. (2021) The HealthChain blockchain for electronic health records: Development study. Journal of Medical Internet Research, 23(1): e13556.
[17] Androulaki, E., Barger, A., Bortnikov, V., et al. (2018) Hyperledger Fabric: A distributed operating system for permissioned blockchains. arXiv preprint arXiv: 1801.10228.