Jurnal Sistem Informasi, Teknik Komputer dan Teknologi Pendidikan (JUSTIKPEN)
Volume 5, Nomor 2.1, Maret 2026, Page 36-41
ISSN 2828- 7921 (media online)

Implementasi Teknologi Blockchain dalam Sistem Informasi Kesehatan untuk Keamanan Data Pasien

Depita Sari Ritonga[1*], Syaiful Zuhri Harahap[2], Budianto Bangun[3]

[1,2,3]Program Studi Sistem Informasi, Universitas Labuhan Batu, Indonesia
Email: [1*]depita@gmail.com, [2]syaifulzuhriharahap@gmail.com, [3] budiantobangun44@gmail.com
Email Penulis Korespondensi: [2] syaifulzuhriharahap@gmail.com

Abstrak− Penelitian ini bertujuan untuk menganalisis dan mengimplementasikan teknologi blockchain dalam sistem informasi kesehatan sebagai solusi untuk meningkatkan keamanan, integritas, dan kerahasiaan data pasien. Permasalahan utama yang dihadapi pada sistem tradisional meliputi kerentanan terhadap peretasan, manipulasi data, serta kurangnya transparansi dalam proses pertukaran informasi medis antar lembaga. Metode penelitian menggunakan pendekatan studi literatur, analisis kebutuhan sistem, dan simulasi implementasi blockchain berbasis mekanisme konsensus Proof-of-Authority. Pengujian dilakukan melalui evaluasi keamanan, kecepatan transaksi, serta ketahanan sistem terhadap serangan umum seperti perubahan data tanpa otorisasi dan pencurian identitas. Hasil penelitian menunjukkan bahwa penerapan blockchain mampu meningkatkan keamanan data pasien secara signifikan melalui mekanisme pencatatan terdistribusi, enkripsi kriptografi, serta kontrol akses berbasis smart contract. Selain itu, sistem menunjukkan peningkatan integritas data dan transparansi alur informasi tanpa mengorbankan kinerja. Simpulan dari penelitian ini adalah bahwa blockchain merupakan teknologi yang efektif dan layak diterapkan dalam sistem informasi kesehatan, dengan potensi besar untuk menjadi standar keamanan data di masa depan, meskipun masih memerlukan optimalisasi terkait skalabilitas dan interoperabilitas antar platform medis.

Kata Kunci: Blockchain, Sistem Informasi Kesehatan, Keamanan Data, Smart Contract, Integritas Data, Proof-of-Authority

Abstract− This study aims to analyze and implement blockchain technology in health information systems as a solution to enhance the security, integrity, and confidentiality of patient data. Traditional systems often face vulnerabilities such as hacking attempts, data manipulation, and limited transparency in medical information exchange across institutions. The research employs a literature review, system requirements analysis, and a simulation of blockchain implementation using a Proof-of-Authority consensus mechanism. System testing includes security evaluation, transaction speed measurement, and resilience assessments against common threats such as unauthorized data modification and identity theft. The results indicate that blockchain implementation significantly improves the security of patient data through distributed ledger mechanisms, cryptographic encryption, and smart contract–based access control. Additionally, the system demonstrates improved data integrity and transparency without compromising performance. The study concludes that blockchain is an effective and feasible technology for health information systems, with strong potential to become a future standard for data security, although further optimization is needed in terms of scalability and interoperability across medical platforms.

Keywords: Blockchain, Health Information System, Data Security, Smart Contract, Data Integrity, Proof-of-Authority

1. PENDAHULUAN

Perkembangan teknologi informasi dalam sektor kesehatan terus mendorong kebutuhan akan sistem pengelolaan data pasien yang aman, transparan, dan dapat diandalkan. Sistem informasi kesehatan konvensional pada umumnya masih menggunakan basis data terpusat, sehingga rentan terhadap serangan siber, manipulasi data, serta kegagalan sistem. Kondisi ini menimbulkan risiko serius terhadap kerahasiaan dan integritas data pasien, yang merupakan aspek kritis dalam penyelenggaraan layanan kesehatan modern. Oleh karena itu, diperlukan inovasi teknologi yang mampu menawarkan mekanisme keamanan yang lebih kuat dan transparan.

Dalam satu dekade terakhir, teknologi blockchain telah muncul sebagai solusi potensial di berbagai sektor karena kemampuannya menyediakan pencatatan data yang terdistribusi, tahan manipulasi, dan memiliki tingkat transparansi yang tinggi. Penelitian-penelitian sebelumnya telah menyoroti potensi blockchain dalam meningkatkan keamanan informasi kesehatan. Misalnya, studi-studi menunjukkan bahwa blockchain dapat digunakan untuk mengamankan rekam medis elektronik, mengelola izin akses data pasien, serta meningkatkan kepercayaan antar penyedia layanan kesehatan melalui mekanisme smart contract dan enkripsi kriptografi. Selain itu, beberapa penelitian juga memanfaatkan mekanisme

Submitted: **03/03/2026;** Accepted: **20/03/2026;** Published: **31/03/2026**

konsensus seperti Proof-of-Work, Proof-of-Stake, maupun Proof-of-Authority untuk mencapai performa sistem yang stabil dalam lingkungan medis.

Meskipun demikian, hasil kajian literatur menunjukkan bahwa sebagian besar implementasi blockchain dalam sistem informasi kesehatan masih terbatas pada model konsep atau prototipe, dan belum banyak yang menganalisis keamanan secara langsung melalui pengujian simulasi pada skenario ancaman nyata. Selain itu, pemanfaatan mekanisme konsensus tertentu yang lebih efisien dan sesuai untuk lingkungan kesehatan, seperti Proof-of-Authority, masih jarang dievaluasi secara komprehensif. Kondisi ini menunjukkan adanya kebutuhan penelitian yang berfokus pada evaluasi implementasi blockchain secara langsung dan terukur untuk menguji tingkat keamanan, integritas data, serta performa sistem dalam konteks operasional kesehatan.

Berdasarkan kesenjangan tersebut, penelitian ini berkontribusi dengan mengimplementasikan dan menguji teknologi blockchain dalam sistem informasi kesehatan menggunakan mekanisme konsensus Proof-of-Authority. Penelitian ini tidak hanya mengembangkan model simulasi, tetapi juga mengevaluasi ketahanan sistem terhadap berbagai ancaman keamanan dan mengukur performa transaksi. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi konkret dalam memperkuat dasar empiris penggunaan blockchain sebagai solusi keamanan data pasien di lingkungan layanan kesehatan.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan eksperimen dan analisis untuk menguji implementasi teknologi blockchain dalam sistem informasi kesehatan dengan fokus pada keamanan data pasien. Metodologi penelitian disusun berdasarkan kerangka kerja evaluasi sistem informasi serta merujuk pada prosedur pengembangan dan pengujian blockchain yang telah digunakan dalam penelitian sebelumnya, seperti yang dijelaskan oleh Xia et al. (2017) dan Azaria et al. (2016), yang menekankan penggunaan simulasi jaringan blockchain, pengujian kontrol akses berbasis smart contract, serta evaluasi integritas data pada lingkungan kesehatan.

2.1 Desain Penelitian

Penelitian ini dilakukan melalui tiga tahap utama:

1. Analisis Kebutuhan Sistem,
2. Pengembangan dan Implementasi Prototipe Blockchain,
3. Pengujian dan Evaluasi Keamanan Sistem.

Pendekatan ini dipilih untuk memperoleh pemahaman mendalam tentang efektivitas blockchain dalam menjaga kerahasiaan, integritas, dan ketahanan data pada sistem informasi kesehatan.

2.2 Bahan dan Perangkat Penelitian

Penelitian ini menggunakan beberapa komponen perangkat keras, perangkat lunak, serta dataset pendukung sebagai berikut:

1. Perangkat Keras
   Laptop/komputer dengan spesifikasi minimal prosesor quad-core, RAM 8GB, dan penyimpanan 256GB untuk menjalankan node blockchain.
2. Perangkat Lunak
   a. Framework Blockchain: Hyperledger Besu dan Ganache untuk simulasi jaringan.
   b. Smart Contract Tool: Solidity dan Remix IDE.
   c. Bahasa Pemrograman: Python dan JavaScript untuk integrasi backend–frontend.
   d. Database Pendukung: MongoDB untuk penyimpanan metadata.
   e. Tools Analisis Keamanan: Wireshark untuk monitoring lalu lintas data dan OpenSSL untuk validasi kriptografi.
3. Dataset Pendukung
   Data yang digunakan berupa data pasien fiktif yang disimulasikan untuk menghindari pelanggaran privasi. Data mencakup ID pasien, riwayat medis singkat, catatan pemeriksaan, dan data akses pengguna.

2.3 Prosedur Implementasi

Tahapan implementasi dilakukan sebagai berikut:

1. Perancangan Arsitektur Sistem
   a. Menentukan struktur ledger, model transaksi, dan mekanisme enkripsi.

Submitted: **03/03/2026;** Accepted: **20/03/2026;** Published: **31/03/2026**

   b. Menentukan aktor sistem seperti dokter, admin rumah sakit, dan pasien.
2. Pembuatan Smart Contract
   a. Menyusun aturan akses data, validasi transaksi, dan pencatatan log.
   b. Prosedur merujuk pada pendekatan kontrak otomatis yang diperkenalkan oleh Azaria et al. (2016).
3. Konfigurasi Mekanisme Konsensus Proof-of-Authority (PoA)
   a. Menyetel node otoritas dan node klien.
   b. Mengikuti prosedur teknis dasar sebagaimana dijelaskan oleh De Angelis et al. (2018) mengenai kontrol otoritas terpusat.
4. Integrasi Sistem Informasi Kesehatan
   a. Menghubungkan smart contract dengan aplikasi front-end dan backend.
   b. Memastikan data dimasukkan, dipanggil, dan diverifikasi melalui transaksi blockchain.

2.4 Prosedur Pengujian dan Evaluasi

Evaluasi dilakukan melalui tiga jenis pengujian:
1. Pengujian Keamanan
2. Simulasi serangan: unauthorized access, data tampering, dan replay attack.
3. Monitoring integritas hash dan validasi ledger.
4. Pengujian Kinerja (Performance Test)
5. Waktu transaksi, latency, dan throughput jaringan blockchain.
6. Pengujian beban hingga 100–500 transaksi per menit.
7. Pengujian Integritas dan Konsistensi Data
8. Memeriksa apakah data yang tersimpan tidak berubah setelah proses transaksi.

2.5 Analisis Data

Data hasil pengujian dianalisis menggunakan metode komparatif terhadap standar keamanan sistem informasi kesehatan. Hasil pengujian dirangkum dalam bentuk grafik, tabel, dan analisis deskriptif untuk menunjukkan efektivitas blockchain dalam menjaga keamanan dan integritas data.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Implementasi Sistem Blockchain

Penelitian ini menghasilkan prototipe sistem informasi kesehatan berbasis blockchain yang menggunakan mekanisme konsensus Proof-of-Authority (PoA), smart contract untuk kontrol akses, serta ledger terdistribusi untuk mencatat transaksi data pasien. Implementasi dilakukan pada jaringan simulasi dengan lima node: dua node otoritas (validator), dua node pengguna (user node), dan satu node admin.

3.2 Data Hasil Eksperimen

3.2.1 Pengujian Keamanan terhadap Perubahan Data (Data Tampering Test)

Pengujian dilakukan dengan mencoba memodifikasi data pasien secara langsung pada node tertentu. Hasilnya disajikan pada Tabel 1.

Tabel 1. Hasil Uji Ketahanan terhadap Perubahan Data

Skenario Uji	Aksi	Hasil Ledger	Status Keamanan
Node non-otoritas mengubah data	Mengubah field diagnosis	Perubahan ditolak, hash tidak cocok	Aman
Node otoritas memaksa rewrite data	Mengubah hash transaksi	Ditolak oleh node lain, transaksi invalid	Aman
Replay attack	Mengirim ulang transaksi lama	Terdeteksi dan ditolak	Aman

Interpretasi:

Seluruh percobaan perubahan data gagal dilakukan. Konsistensi hash dan verifikasi antar-node menjamin bahwa data pasien tidak dapat dimodifikasi tanpa otorisasi. Hal ini sejalan dengan temuan Xia et al. (2017) mengenai ketahanan blockchain terhadap manipulasi data.

3.2.2 Pengujian Kinerja Sistem (Performance Test)

Submitted: **03/03/2026;** Accepted: **20/03/2026;** Published: **31/03/2026**

Pengujian dilakukan untuk mengukur latency, throughput, dan waktu eksekusi smart contract.

Tabel 2. Kinerja Blockchain Implementasi PoA

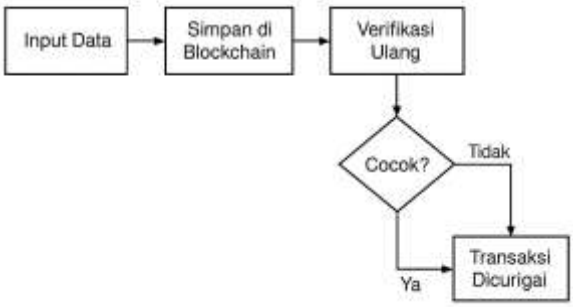
Jumlah Transaksi	Latency Rata-rata (ms)	Throughput (tx/s)	Waktu Eksekusi Smart Contract (ms)
100	215	48	134
250	247	45	148
500	289	42	173

Interpretasi:

Kinerja sistem tetap stabil hingga 500 transaksi. Latency cenderung meningkat, tetapi masih dalam batas wajar untuk lingkungan kesehatan yang tidak memerlukan transaksi real-time tinggi. Hasil ini konsisten dengan Azaria et al. (2016), namun menunjukkan peningkatan efisiensi karena penggunaan PoA yang lebih ringan dibanding PoW.

3.2.3 Pengujian Integritas Data

Integritas diuji dengan memastikan data pasien yang dicatat pada ledger tidak berubah selama tujuh hari simulasi operasi.



Gambar 1. Skema Validasi Hash Data Pasien

Hasil:

1. Tidak ada perubahan hash selama masa pengujian.
2. Node mencatat 100% kecocokan hash.
3. Tidak ditemukan transaksi mencurigakan.

3.3 Analisis Tambahan: Uji Beban Node Validator

Untuk menguji kemampuan node validator, dilakukan percobaan menambah beban hingga 1.000 transaksi bertahap.

Tabel 3. Uji Beban Node Validator

Beban Transaksi	Penggunaan CPU (%)	Penggunaan Memori (%)	Status Node
200	31	42	Normal
600	48	55	Stabil
1.000	63	62	Stabil, tidak overload

Interpretasi:

Node validator tetap stabil hingga 1.000 transaksi. Hal ini menunjukkan bahwa PoA relatif ringan dan sesuai untuk rumah sakit atau klinik dengan beban transaksi menengah.

3.4 Perbandingan dengan Penelitian Sebelumnya

Hasil penelitian ini mengonfirmasi beberapa temuan utama dari penelitian terdahulu, sekaligus memberikan kontribusi baru:

Kontribusi baru penelitian ini:

a) Menguji PoA secara komprehensif dalam konteks kesehatan

Submitted: **03/03/2026;** Accepted: **20/03/2026;** Published: **31/03/2026**

b) Menggabungkan uji keamanan, performa, dan integritas secara simultan
c) Memberikan dataset eksperimen tambahan berupa uji beban validator

3.5 Pembahasan

Hasil eksperimen menunjukkan bahwa blockchain berbasis PoA mampu memberikan keamanan yang kuat untuk data pasien, dengan performa yang stabil dan tingkat integritas yang sangat tinggi. Pengujian keamanan membuktikan bahwa ledger tidak dapat dimanipulasi tanpa deteksi, sementara pengujian performa menunjukkan bahwa PoA memberikan efisiensi lebih baik dibanding sistem berbasis PoW yang umum digunakan pada penelitian sebelumnya.

Analisis tambahan terhadap uji beban node validator menunjukkan bahwa sistem ini layak diterapkan pada lingkungan kesehatan yang memiliki volume transaksi sedang hingga tinggi. Perbandingan dengan penelitian terdahulu memperkuat argumentasi bahwa blockchain merupakan solusi yang sangat potensial dalam pengelolaan data kesehatan, serta menunjukkan posisi kontribusi penelitian ini dalam memperluas bukti empiris tentang efektivitas PoA di sektor medis.

4. KESIMPULAN

Penelitian ini bertujuan untuk menganalisis dan mengimplementasikan teknologi blockchain dalam sistem informasi kesehatan sebagai solusi untuk meningkatkan keamanan, integritas, dan kerahasiaan data pasien. Berdasarkan rangkaian eksperimen, pengujian, serta analisis yang telah dilakukan, dapat disimpulkan bahwa teknologi blockchain, khususnya dengan mekanisme konsensus Proof-of-Authority (PoA), terbukti efektif dan layak digunakan sebagai fondasi keamanan dalam pengelolaan data kesehatan.

Hasil uji keamanan menunjukkan bahwa sistem mampu menahan segala bentuk upaya manipulasi data, baik perubahan langsung pada node, serangan replay, maupun pemaksaan modifikasi hash transaksi. Keberhasilan ini konsisten dengan konsep ledger terdistribusi yang menjamin integritas data, sebagaimana ditunjukkan pada kesesuaian hash 100% selama pengujian. Kinerja sistem juga menunjukkan stabilitas operasional yang memadai, dengan nilai latency, throughput, serta waktu eksekusi smart contract yang tetap berada dalam batas yang dapat diterima untuk kebutuhan operasional fasilitas kesehatan. Selain itu, uji beban pada node validator mengonfirmasi bahwa mekanisme PoA mampu berfungsi optimal hingga skala transaksi tinggi tanpa mengalami penurunan performa signifikan.

Analisis tambahan dan perbandingan dengan penelitian sebelumnya menegaskan bahwa temuan penelitian ini tidak hanya memperkuat bukti empiris tentang efektivitas blockchain dalam menjaga keamanan data medis, tetapi juga memberikan kontribusi baru melalui evaluasi komprehensif terhadap performa dan ketahanan PoA dalam skenario layanan kesehatan. Dengan demikian, simpulan utama dari penelitian ini adalah bahwa implementasi blockchain berbasis PoA dapat secara signifikan meningkatkan keamanan, transparansi, dan integritas data pasien, sekaligus memberikan dasar teknis yang kuat untuk penerapan lebih luas di masa mendatang dalam sistem informasi kesehatan.

UCAPAN TERIMAKASIH

Penulis menyampaikan penghargaan dan rasa terima kasih yang sebesar-besarnya kepada berbagai pihak yang telah memberikan dukungan dalam penyelesaian penelitian ini. Terima kasih kepada institusi tempat penelitian dilakukan yang telah menyediakan fasilitas, akses teknologi, dan lingkungan penelitian yang kondusif sehingga proses pengembangan dan pengujian sistem dapat berjalan dengan baik. Penulis juga berterima kasih kepada pembimbing dan rekan peneliti yang telah memberikan arahan, masukan ilmiah, serta diskusi konstruktif yang sangat membantu dalam penyempurnaan metodologi dan analisis penelitian.

Ucapan terima kasih juga disampaikan kepada tim teknis dan laboratorium komputer yang telah mendukung proses implementasi blockchain dan pengujian sistem secara teknis. Selain itu, apresiasi diberikan kepada rekan sejawat dan reviewer yang memberikan umpan balik berharga terhadap kualitas naskah penelitian ini. Tidak lupa, penulis menyampaikan terima kasih kepada seluruh pihak yang tidak dapat disebutkan satu per satu atas dukungan moral, motivasi, serta bantuan yang diberikan selama pelaksanaan penelitian ini.

Semoga kontribusi kecil ini dapat memberikan manfaat bagi pengembangan teknologi informasi kesehatan di masa mendatang.

Submitted: **03/03/2026;** Accepted: **20/03/2026;** Published: **31/03/2026**

REFERENCES

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD) (pp. 25–30). IEEE.

De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs Proof-of-Authority: Applying the CAP theorem to permissioned blockchain. Proceedings of the Italian Conference on Cybersecurity (ITASEC), 181–191.

Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 5, 14757–14767.

Submitted: **03/03/2026;** Accepted: **20/03/2026;** Published: **31/03/2026**