



Penerapan Teknologi Blockchain Pada Keamanan dan Transparansi Penyimpanan Data Medis Pasien

Richelle Vania Thionanda¹, Valencia Sutio², Maria Stephanie Rayadi³, Stefanie Wijaya⁴, Youko Tumiwa⁵, Joosten⁶

^{1,2,3,4,5,6} Program Studi Sistem Informasi, Fakultas Informatika

Universitas Mikroskil, Sumatera Utara, Indonesia

E-mail : 221121499@students.mikroskil.ac.id

Article Info

Article history:

Received October 08, 2025

Revised October 12, 2025

Accepted October 17, 2025

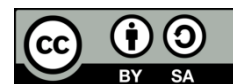
Keywords:

Blockchain, Medical Data, Security, Transparency, Digital Health System

ABSTRACT

Blockchain technology emerges as an innovative solution to enhance the security and transparency of patient medical data storage. This decentralized system employs encryption mechanisms and smart contracts to ensure data integrity and authenticity without relying on a single authority. The application of blockchain in the healthcare sector can address issues such as data breaches, medical record duplication, and limited access among healthcare institutions. Through models like BigchainDB and Hyperledger, medical data can be managed securely, efficiently, and auditable by authorized parties. Despite challenges related to network scalability, infrastructure costs, and regulatory readiness, blockchain holds great potential to support a secure, integrated, and patient-centered digital health system. With strong policy support and cross-sector collaboration, blockchain can serve as a foundational pillar for digital transformation in the healthcare industry.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Article Info

Article history:

Received October 08, 2025

Revised October 12, 2025

Accepted October 17, 2025

Keywords:

Blockchain, Data Medis, Keamanan, Transparansi, Sistem Kesehatan Digital

ABSTRAK

Teknologi blockchain hadir sebagai solusi inovatif dalam meningkatkan keamanan dan transparansi penyimpanan data medis pasien. Sistem ini bekerja secara desentralisasi dengan mekanisme enkripsi dan *smart contract* yang memastikan integritas serta keaslian data tanpa bergantung pada otoritas tunggal. Penerapan blockchain di sektor kesehatan dapat mengatasi permasalahan kebocoran data, duplikasi rekam medis, serta keterbatasan akses antar lembaga kesehatan. Melalui model seperti BigchainDB dan Hyperledger, data medis dapat dikelola secara aman, efisien, dan mudah diaudit oleh pihak berwenang. Meskipun masih menghadapi tantangan, seperti skalabilitas jaringan, biaya infrastruktur, dan kesiapan regulasi, teknologi ini memiliki potensi besar untuk mendukung sistem kesehatan digital yang aman, terintegrasi, dan berorientasi pada pasien. Dengan dukungan kebijakan serta kolaborasi lintas sektor, blockchain dapat menjadi fondasi utama transformasi digital di bidang kesehatan.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



**Corresponding Author:**

Richelle Vania Thionanda

Universitas Mikroskil

221121499@students.mikroskil.ac.id**PENDAHULUAN**

Perkembangan teknologi informasi dalam sepuluh tahun terakhir telah memberikan pengaruh besar pada dunia kesehatan, terutama dalam sistem pengelolaan rekam medis pasien. Peralihan dari sistem berbasis kertas ke dalam bentuk *Rekam Medis Elektronik (RME)* merupakan perubahan utama yang bertujuan untuk meningkatkan efisiensi layanan, aksesibilitas data, dan akurasi informasi medis. Digitalisasi ini diharapkan mampu mempercepat proses pengambilan keputusan klinis dan meningkatkan kerja sama antara profesional kesehatan. Namun, di balik keuntungan tersebut, terdapat masalah serius terkait keamanan, privasi, dan transparansi data pasien. (Ramadahni, 2024) menekankan bahwa ancaman terhadap serangan siber serta kemungkinan kebocoran data masih menjadi masalah utama dalam penerapan RME. Di Indonesia, kasus kebocoran data pribadi, termasuk informasi kesehatan, semakin meningkat, yang menunjukkan betapa pentingnya perlindungan data medis dengan pendekatan teknologi yang lebih handal.

Salah satu teknologi yang banyak dibahas sebagai solusinya adalah blockchain. Karakteristiknya yang terdesentralisasi, tidak dapat dimodifikasi, dan transparan dianggap dapat meningkatkan integritas serta membangun kepercayaan dalam pengelolaan data medis. Penelitian oleh (Tampubolon et al., 2022) membuktikan bahwa penerapan blockchain berbasis BigchainDB dalam sistem RME dapat menjamin keamanan data sekaligus menyediakan mekanisme audit yang jelas. Sementara itu, (Suryawijaya, 2023) mencatat bahwa blockchain sangat relevan dalam konteks perlindungan data karena sifatnya yang terdistribusi dan sulit untuk dimanipulasi. Hasil-hasil tersebut menunjukkan potensi besar blockchain dalam menjawab isu keamanan data medis, meskipun hingga kini penerapannya masih banyak berhenti pada tahap konseptual.

Walaupun menjanjikan, penelitian sebelumnya belum sepenuhnya mengatasi kompleksitas yang ada di dunia nyata. Pertama, sebagian besar studi hanya berfokus pada desain sistem dan uji coba dalam skala kecil tanpa penerapan nyata di rumah sakit, sehingga kurang mampu dalam menjelaskan interoperabilitas antar fasilitas (Hamidah et al., 2024). Kedua, aspek regulasi, terutama *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi* (Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, 2022), masih jarang dijadikan bahan analisis, padahal UU tersebut menegaskan prinsip akuntabilitas, transparansi, serta hak pasien atas data pribadinya. Ketiga, masalah teknis seperti pengelolaan kunci enkripsi dan biaya untuk implementasi blockchain dalam skala besar belum dibahas secara menyeluruh. Kondisi ini menunjukkan adanya kesenjangan riset yang perlu ditangani melalui pendekatan yang lebih komprehensif.

Penelitian ini bertujuan untuk menjawab kesenjangan tersebut dengan merancang arsitektur RME yang menggunakan blockchain *hybrid*. Dalam rancangan ini, data medis sensitif disimpan secara terenkripsi di repositori *off-chain*, sementara *hash* dan log transaksi dicatat di blockchain untuk menjamin integritas dan auditabilitas. Selain itu, penelitian ini



juga menyoroti penggunaan *smart contract* untuk manajemen persetujuan (*consent management*), yang memberi pasien lebih banyak kendali terhadap akses dan penggunaan data medis mereka.

Dengan demikian, penelitian ini menjadikan isu fragmentasi data, lemahnya *audit trail*, dan tingginya risiko pelanggaran privasi sebagai dasar dalam merumuskan solusi. Sasaran utamanya adalah menghadirkan kerangka arsitektur RME berbasis blockchain yang dapat diimplementasikan di fasilitas kesehatan di Indonesia, sekaligus memberikan kontribusi akademis dalam bentuk desain teknis yang aplikatif dan mematuhi regulasi. Pendekatan ini diharapkan dapat memperkuat keamanan data serta sejalan dengan kebijakan perlindungan data medis pasien.

TINJAUAN LITERATUR

Teknologi Blockchain dalam Konteks Keamanan dan Transparansi Data Medis

Teknologi Blockchain merupakan teknologi penyimpanan dan pencatatan data yang berpotensi besar dalam mengatasi masalah privasi, interoperabilitas, dan manajemen riwayat medis pasien. Dalam sektor kesehatan, blockchain berperan penting dalam meningkatkan keamanan dan privasi data melalui sistem terdistribusi yang sulit dimanipulasi (Kamaruddin et al., 2024). Platform seperti BigchainDB mendukung *Role-Based Access Control* (RBAC), yang memastikan hanya pihak berwenang seperti dokter, rumah sakit, atau pasien dapat mengakses data sesuai kewenangannya, sehingga privasi lebih terjaga. Berbagai studi menunjukkan blockchain telah berhasil diterapkan pada rekam medis elektronik (EMR), manajemen rantai pasok obat, hingga pemantauan pasien jarak jauh, menandakan penerapannya bersifat praktis dan adaptif (Ramadahni, 2024).

Selain itu, sistem seperti MedRec, Medicalchain, dan Hyperledger terbukti efektif dalam pengelolaan hak akses pasien secara aman dan transparan (Syukurillah et al., 2024). Studi lain juga membuktikan bahwa penerapan BigchainDB menghadirkan solusi desentralisasi, sehingga data medis tidak lagi bergantung pada satu server pusat dan lebih tahan terhadap serangan maupun kehilangan data (Tampubolon et al., 2022).

Arsitektur dan Alur Data

Arsitektur sistem blockchain untuk penyimpanan data medis umumnya terdiri atas node-node yang saling terhubung secara *peer-to-peer*, penyimpanan terdistribusi, enkripsi data, serta *smart contract* yang mengatur izin akses dan validasi transaksi. Setiap data medis pasien, seperti hasil laboratorium atau resep obat, diproses sebagai transaksi baru yang diverifikasi melalui mekanisme konsensus sebelum disimpan dalam blok permanen yang tidak dapat diubah (Syukurillah et al., 2024). Dalam implementasi BigchainDB, setiap transaksi medis diverifikasi terlebih dahulu untuk menjamin integritas data, karena setiap perubahan pada blok akan terdeteksi oleh seluruh node jaringan. Pasien memiliki kunci digital pribadi yang memberi mereka kendali penuh terhadap siapa yang dapat mengakses catatan medisnya (Ramadahni, 2024). Umumnya, sistem kesehatan mengadopsi *Private Blockchain* atau *Consortium (Hybrid) Blockchain* guna membatasi akses hanya kepada pihak berwenang seperti dokter, rumah sakit, dan pasien. Beberapa rancangan arsitektur mengombinasikan *Proof-of-Work* (PoW) dengan



kriptografi SHA-256 guna meningkatkan keamanan enkripsi. Sementara itu, alternatif seperti *BigchainDB* menawarkan mekanisme modifikasi terkontrol yang memberikan fleksibilitas lebih besar bagi sistem medis yang bersifat dinamis (Alexander et al., 2025).

Pihak-pihak yang Terlibat

Dalam penerapan blockchain di bidang kesehatan, ada beberapa aktor utama yang terlibat. Pertama, pasien sebagai pemilik data yang memiliki kendali terhadap siapa saja yang boleh mengakses rekam medis mereka, sebagai pemilik data, pasien memiliki kendali yang lebih besar atas informasi kesehatan mereka dan dapat menentukan siapa saja yang diizinkan untuk mengakses catatan medisnya melalui penggunaan kunci kriptografi pribadi atau token akses (Wikarsa et al., 2022). Kedua, tenaga medis (dokter, perawat) yang berperan sebagai pihak yang mencatat, memperbarui, dan membaca data pasien. Ketiga, rumah sakit atau fasilitas kesehatan yang bertindak sebagai penyedia layanan dan pengelola sistem. Keempat, regulator atau pemerintah yang memastikan penerapan sesuai dengan regulasi perlindungan data, seperti UU PDP di Indonesia. Kolaborasi antar pihak ini menjadi penting agar sistem blockchain tidak hanya aman, tetapi juga sesuai dengan kebutuhan operasional layanan kesehatan (Ramadahni, 2024).

Contoh Implementasi

Berbagai studi telah menunjukkan keberhasilan penerapan blockchain di sektor kesehatan, seperti pemanfaatan *Hyperledger* dan *BigchainDB* untuk sistem rekam medis terdesentralisasi (Tampubolon et al., 2022). Penerapan lain mencakup Electronic Medical Record (EMR), pertukaran data antar rumah sakit, manajemen uji klinis, dan sistem klaim asuransi (Ramadahni, 2024). Model seperti SEMRES menerapkan enkripsi ganda (AES dan RSA) untuk menjaga keamanan data, sedangkan sistem PcBEHR memberikan kontrol penuh kepada pasien melalui integrasi blockchain dengan *InterPlanetary File System* (IPFS). Selain itu, integrasi blockchain dengan *Internet of Medical Things* (IoMT) juga dikembangkan untuk memantau pasien jarak jauh secara aman (Syukurillah et al., 2024). Implementasi blockchain pada rantai pasok obat juga memungkinkan pelacakan asal-usul obat dari produsen hingga pasien, sehingga meminimalisir risiko pemalsuan dan meningkatkan transparansi distribusi farmasi.

Manfaat

Penggunaan blockchain pada rekam medis meningkatkan keamanan, transparansi, dan privasi data pasien. Dari sisi keamanan, catatan medis tidak dapat dimodifikasi secara ilegal, sementara transparansi terjamin karena setiap transaksi terekam dan dapat diaudit. Mekanisme enkripsi dan kontrol akses menjaga kepemilikan data tetap di tangan pasien. Selain itu, sifat terdistribusi blockchain mempermudah interoperabilitas antar sistem rumah sakit, sehingga meningkatkan kualitas layanan, mengurangi kesalahan medis, dan menumbuhkan kepercayaan pasien terhadap sistem digital (Ramadahni, 2024). Studi lain juga menegaskan bahwa blockchain dapat meningkatkan efisiensi biaya dengan mengurangi duplikasi pemeriksaan medis dan mempercepat proses klaim asuransi (Syukurillah et al., 2024).



Keterbatasan

Meskipun menjanjikan, penerapan blockchain dalam catatan medis masih menghadapi sejumlah tantangan utama. Pertama, keterbatasan skalabilitas, di mana sistem sulit menangani volume transaksi besar secara efisien (Tampubolon et al., 2022). Kedua, kebutuhan infrastruktur dan biaya implementasi yang tinggi, khususnya bagi rumah sakit kecil. Ketiga, belum adanya standar dan regulasi global yang seragam, sehingga menghambat interoperabilitas lintas negara (Ramadahni, 2024). Keempat, keterbatasan literasi teknologi tenaga medis dan pasien menjadi penghalang adopsi. Dengan demikian, penerapan blockchain memerlukan penyesuaian teknis, kebijakan, serta edukasi berkelanjutan agar manfaatnya dapat dioptimalkan (Syukurillah et al., 2024).

Arah Penelitian Selanjutnya

Penelitian mendatang perlu memperdalam integrasi blockchain dengan IoMT dan sistem pemantauan kesehatan real-time. Sistem seperti EHRGuard yang memanfaatkan data sensor medis dalam blockchain terbukti meningkatkan keamanan dan interoperabilitas (Othman et al., 2025). Selanjutnya, pengembangan skema seperti SCALHEALTH memanfaatkan struktur paralel blockchain + IPFS menawarkan potensi skalabilitas tinggi untuk aplikasi kesehatan berskala luas (Mohammadi et al., 2024).

Konsep *federated learning* dapat menjaga privasi data antar institusi tanpa memusatkan data mentah (Samantray et al., 2025). Selain aspek teknis, penelitian mengenai model blockchain yang hemat energi (seperti PoS atau algoritma ringan) dan kepatuhan regulatif (terkait UU PDP) menjadi sangat penting agar sistem yang dirancang tidak hanya aman, tetapi juga berkelanjutan dan legal di Indonesia. Integrasi dengan AI dan *deep learning* dapat meningkatkan deteksi anomali serta efisiensi pengelolaan data medis, dengan dukungan *off-chain storage* dan *permissioned blockchain* yang adaptif (Ali et al., 2023). Dengan demikian, arah penelitian di masa depan dapat berfokus pada pengembangan arsitektur blockchain yang aman, terdistribusi, dan berdaya guna tinggi, sekaligus mendukung transformasi digital sektor kesehatan yang terintegrasi.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode Systematic Literature Review (SLR) dan perancangan arsitektur sistem, bertujuan menganalisis tantangan dan potensi penerapan blockchain dalam penyimpanan data medis, tanpa eksperimen langsung (Lincopinis et al., 2024).

Tahapan penelitian dilakukan sebagai berikut:

1. Identifikasi dan pengumpulan literatur dilakukan melalui database ilmiah bereputasi seperti IEEE Xplore, ScienceDirect, SpringerLink, dan MDPI, menggunakan kata kunci “*blockchain healthcare*”, “*electronic medical record*”, “*data privacy*”, dan “*scalability blockchain*”. Artikel yang dipilih merupakan publikasi tahun 2022–2025, berbahasa Inggris, dan telah melalui proses *peer review*, serta relevan dengan bidang kesehatan digital dan tata kelola data medis (Kamaruddin et al., 2024). Dari hasil pencarian awal



- sebanyak kurang lebih 80 artikel, sebanyak 25 artikel diseleksi lebih lanjut sesuai kriteria kelayakan untuk dianalisis.
2. Seleksi dan analisis isi (content analysis) dilakukan untuk mengidentifikasi isu utama seperti skalabilitas, privasi data, efisiensi biaya, interoperabilitas, dan kepatuhan regulatif (Tawfik et al., 2025b). Setiap artikel dikodekan secara manual untuk mengekstraksi insight yang relevan bagi rancangan arsitektur sistem blockchain di sektor kesehatan.
 3. Sintesis hasil kajian digunakan untuk merumuskan rancangan arsitektur sistem blockchain hybrid, yang menggabungkan penyimpanan on-chain (metadata, hash, log akses) dan off-chain (data medis terenkripsi) serta model konseptual penerapan di rumah sakit Indonesia (Singh et al., 2025).
 4. Analisis regulatif dan kontekstual dilakukan dengan meninjau kesesuaian rancangan terhadap Peraturan Menteri Kesehatan No. 24 Tahun 2022 tentang Rekam Medis Elektronik dan Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Analisis ini dilakukan secara kualitatif dengan menilai sejauh mana komponen blockchain mendukung kepatuhan terhadap prinsip privasi, keamanan, dan hak kepemilikan data medis (Pratiwi et al., 2025).

Metode ini memastikan bahwa rancangan arsitektur yang dihasilkan memiliki dasar ilmiah yang kuat, kontekstual terhadap regulasi nasional, serta potensial untuk diimplementasikan secara praktis dalam ekosistem kesehatan digital Indonesia.

HASIL DAN PEMBAHASAN

Penerapan teknologi blockchain dalam penyimpanan data medis memiliki potensi besar untuk meningkatkan keamanan, transparansi, dan efisiensi pengelolaan Rekam Medis Elektronik (RME). Meski demikian, tantangan tetap muncul terkait skalabilitas, privasi, kepatuhan regulasi, dan biaya implementasi. Pembahasan berikut menyoroti keempat aspek tersebut secara mendalam, sekaligus memberikan temuan dan rekomendasi untuk implementasi yang sesuai dengan konteks sistem kesehatan di Indonesia.

Skalabilitas

Skalabilitas menjadi salah satu tantangan utama karena volume dan kompleksitas data medis sangat besar, mencakup catatan elektronik, hasil laboratorium, dan data sensor real-time. Penyimpanan langsung di blockchain memperlambat sinkronisasi antar-node dan meningkatkan kebutuhan sumber daya (Lincopinis et al., 2024). Selain itu, blockchain publik seperti Ethereum atau Bitcoin umumnya hanya mampu memproses puluhan transaksi per detik, jauh di bawah kebutuhan sistem kesehatan (Abdelsalam, 2023).

Solusi yang banyak diusulkan mencakup *multi-layered architecture*, *sharding*, dan *sidechain* (Javan et al., 2024). Implementasi *permissioned* blockchain seperti *Hyperledger* terbukti lebih efisien, sementara pendekatan hybrid on-chain/off-chain menjaga integritas data tanpa membebani penyimpanan (J et al., 2023). Integrasi teknologi kecerdasan buatan (AI) dapat meningkatkan efisiensi beban komputasi antar-node hingga 25% (Ali et al., 2023). Namun demikian, keberhasilan peningkatan skalabilitas blockchain tetap bergantung pada kesiapan infrastruktur dan kolaborasi antar lembaga (Singh et al., 2025).



Privasi

Aspek privasi merupakan isu krusial karena data medis termasuk kategori sensitif. Blockchain bersifat transparan dan immutable, sehingga berpotensi menimbulkan risiko kebocoran data (SIP Law Firm, 2025). Meskipun data terenkripsi, metadata tetap dapat dianalisis untuk melacak identitas pasien (Kamaruddin et al., 2024).

Untuk mengurangi risiko tersebut, sebagian besar penelitian menyarankan penggunaan arsitektur hybrid, yakni memisahkan data utama dan data verifikasi. Dalam pendekatan ini, data medis asli disimpan secara *off-chain* pada server rumah sakit atau jaringan IPFS (*InterPlanetary File System*), sedangkan blockchain hanya mencatat *hash* atau *pointer* dari data tersebut. (Tawfik et al., 2025a). Penggunaan enkripsi asimetris dan *smart contract* berbasis kontrol akses memungkinkan pasien mengatur hak akses terhadap datanya.

Selain persoalan teknis, isu privasi juga erat kaitannya dengan kepatuhan terhadap regulasi perlindungan data pribadi di berbagai negara. Kepatuhan terhadap HIPAA, GDPR, dan UU PDP 2022 juga penting karena blockchain yang immutable bertentangan dengan prinsip *right to erasure*. Solusi seperti penyimpanan hash pointer di blockchain memungkinkan penghapusan data tanpa merusak integritas catatan (Pratiwi et al., 2025). Selain itu, teknologi Zero-Knowledge Proof (ZKP) dan Homomorphic Encryption dapat menjaga keseimbangan antara privasi dan transparansi (Kamaruddin et al., 2024). Secara keseluruhan, pengelolaan privasi dalam blockchain kesehatan membutuhkan keseimbangan antara keamanan, integritas data, dan hak privasi pasien. Melalui kombinasi pendekatan teknis, seperti enkripsi, penyimpanan off-chain, dan kontrol akses berbasis smart contract, serta kepatuhan terhadap kerangka hukum nasional maupun internasional, blockchain dapat menjadi solusi yang efektif untuk menjamin keamanan data medis tanpa melanggar hak-hak privasi pasien.

Regulasi

Regulasi penerapan teknologi blockchain dalam pengelolaan dan penyimpanan data medis di Indonesia masih dalam tahap awal dan belum memiliki aturan khusus. Implementasinya perlu diselaraskan dengan Permenkes No. 24 Tahun 2022 dan UU Pelindungan Data Pribadi (UU PDP) 2022, yang menekankan aspek keamanan, integritas, dan hak subjek data. Tantangan muncul karena sifat *immutable* blockchain berpotensi bertentangan dengan hak penghapusan data pribadi, sehingga pendekatan *off-chain storage* menjadi solusi yang paling sesuai (Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis, 2022).

Selain itu, berbagai regulasi kesehatan nasional mewajibkan penyelenggara sistem informasi kesehatan untuk menjamin kerahasiaan dan integritas data medis, namun masih terdapat kesenjangan standar keamanan antar institusi. Sebagai pembanding, di Amerika Serikat, *Health Insurance Portability and Accountability Act* (HIPAA) telah lama menjadi acuan perlindungan data medis melalui prinsip keamanan, integritas, dan kontrol akses berbasis *smart contract* (HIPAA, n.d.).

Dengan belum adanya pedoman khusus terkait blockchain di sektor kesehatan, tantangan utama Indonesia mencakup kepastian hukum, tanggung jawab pengendali data, dan standar interoperabilitas antar sistem. Oleh karena itu, diperlukan kolaborasi pemerintah,



regulator, dan industri untuk merumuskan kebijakan nasional yang mendukung inovasi blockchain sekaligus menjamin aspek hukum, privasi, dan etika dalam ekosistem kesehatan digital.

Biaya

Penerapan teknologi blockchain pada penyimpanan data medis pasien memerlukan investasi awal yang tinggi untuk pengembangan, infrastruktur, dan pelatihan SDM. Estimasi biaya pengembangan sistem blockchain medis berkisar USD 80.000–150.000 tergantung kompleksitas (Tawfik et al., 2025b). Namun, dalam jangka panjang, blockchain mampu menekan kerugian akibat manipulasi data dan mempercepat interoperabilitas. Strategi paling realistis adalah penerapan *pilot project* berskala kecil atau sistem *hybrid* untuk meminimalkan risiko awal (Mohammed et al., 2023).

Langkah Implementasi Pragmatis

Beberapa langkah ini dirancang untuk dapat diimplementasikan secara bertahap dan realistis dalam lingkungan rumah sakit atau Lembaga Kesehatan

1. Analisis Kebutuhan dan Regulasi

Tahap awal bertujuan untuk menetapkan ruang lingkup serta memastikan kepatuhan terhadap regulasi yang berlaku. Proses ini mencakup identifikasi jenis data medis yang dikelola, seperti rekam medis, hasil laboratorium, citra medis, dan resep. Selanjutnya, perlu dilakukan kajian terhadap regulasi perlindungan data pasien, seperti Permenkes No. 24 Tahun 2022, GDPR, dan HIPAA, guna menjamin kepatuhan hukum. (Ramadahni, 2024).

2. Pemilihan Jenis *Blockchain*

Tahap ini bertujuan untuk menyesuaikan sistem dengan kebutuhan privasi dan efisiensi dalam pengelolaan dataa medis. Langkah-langkah yang dilakukan meliputi pemilihan jenis *permissioned blockchain* (private) seperti Hyperledger Fabric, Quorum, atau Corda agar akses data dapat dikendalikan dengan baik. (Akhir et al., 2025).

3. Desain Arsitektur Sistem (Hybrid Model)

Tahap ini bertujuan untuk menyeimbangkan keamanan, efisiensi, dan transparansi dalam pengelolaan data medis berbasis blockchain melalui arsitektur hybrid yang memadukan penyimpanan *on-chain* dan *off-chain*. Pada sisi *on-chain* disimpan metadata, hash file medis, catatan akses, dan izin pasien untuk menjaga transparansi serta jejak audit, sedangkan file medis terenkripsi disimpan di secure database atau cloud storage. Integritas data dijamin melalui pencocokan hash di blockchain, dan keamanan diperkuat dengan algoritma enkripsi AES-256 atau RSA

4. Pengembangan *Smart Contract* (Kontrak Pintar)

Tahap ini bertujuan untuk mengotomatisasi proses pemberian izin dan pencatatan akses terhadap data medis. Implementasinya dilakukan melalui *smart contract* yang mengatur alur hak akses antara pasien, dokter, dan rumah sakit secara terstruktur. Setiap aktivitas akses data akan tercatat otomatis, mencakup informasi tentang siapa yang mengakses, waktu akses, serta alasan penggunaannya, sehingga meningkatkan transparansi dan akuntabilitas. (Akhir et al., 2025).



5. Integrasi dengan Sistem yang Sudah Ada

Tahap ini bertujuan untuk memastikan kompatibilitas dan menjaga kontinuitas operasional antara sistem *blockchain* dengan infrastruktur kesehatan yang sudah ada. Integrasi dilakukan dengan menghubungkan *blockchain* ke *Electronic Health Record* (EHR) dan *Hospital Information System* (HIS) melalui API standar seperti HL7 FHIR, sehingga pertukaran data dapat berlangsung lancar dan sesuai standar internasional (Ramadahni, 2024).

6. *Pilot Project* dan Uji Coba

Tahap ini bertujuan untuk melakukan validasi konsep sekaligus mengidentifikasi potensi risiko sejak tahap awal implementasi. Proses dimulai dengan penerapan sistem pada satu unit rumah sakit atau klinik sebagai proyek percontohan (*pilot project*). Dalam tahap uji coba ini, dilakukan pengujian terhadap beberapa aspek utama, yakni kecepatan akses data, keamanan sistem melalui uji penetrasi, transparansi audit log, serta tingkat kepuasan pengguna yang melibatkan dokter dan pasien. Seluruh hasil evaluasi kemudian didokumentasikan secara sistematis sebagai dasar untuk perbaikan dan penyempurnaan pada versi selanjutnya, sehingga sistem dapat dikembangkan dengan lebih stabil dan efisien.

7. Penguatan Keamanan dan Identitas Digital

Tahap ini bertujuan untuk mencegah terjadinya akses tidak sah serta memastikan integritas dan keaslian data medis. Upaya ini dilakukan dengan menerapkan *Decentralized Identity* (DID) atau sistem identitas berbasis *blockchain* bagi pasien dan tenaga medis, sehingga setiap pengguna memiliki identitas digital yang unik dan terverifikasi. Selain itu, diterapkan *multi-factor authentication* serta tanda tangan digital untuk memperkuat proses otentikasi dan mencegah penyalahgunaan akses. Hanya node yang telah diverifikasi yang diizinkan untuk membaca dan menulis data ke dalam *blockchain*, guna menjaga keamanan jaringan dan mencegah manipulasi informasi (Ramadahni, 2024).

8. Implementasi *Governance* dan Skalibilitas

Tahap ini bertujuan untuk menjamin tata kelola yang baik dan keberlanjutan operasional sistem *blockchain* kesehatan. Langkah pertama dilakukan dengan membentuk *Health Blockchain Consortium* yang berfungsi menetapkan kebijakan terkait akses data, penentuan hak validator, serta mekanisme audit yang transparan. Selanjutnya, disusun SOP pemeliharaan node, mencakup prosedur pembaruan versi sistem dan backup data *off-chain* guna menjaga keandalan serta keamanan informasi. Selain itu, dilakukan *capacity planning* secara berkala untuk mengantisipasi penambahan node baru tanpa mengorbankan performa jaringan, sehingga sistem dapat berkembang secara stabil dan berkelanjutan (Akhir et al., 2025).

9. Pemantauan, Evaluasi, dan Peningkatan Berkelanjutan

Tahap ini bertujuan untuk menjaga efektivitas dan keandalan sistem secara berkelanjutan dengan memanfaatkan *dashboard* pemantauan *real time* untuk mengawasi transaksi dan akses data. Audit berkala terhadap *smart contract* dan node keamanan dilakukan guna mendeteksi kerentanan, sementara umpan balik pengguna dari pasien, dokter, dan administrator digunakan untuk evaluasi kinerja. Sistem juga diperbarui secara rutin agar



selaras dengan perkembangan regulasi dan standar medis terbaru, sehingga tetap relevan, aman, dan efisien dalam mendukung layanan kesehatan (Ramadahni, 2024).

Saran Masa Depan

Sebagai arah penelitian di masa mendatang, penerapan teknologi *blockchain* untuk meningkatkan keamanan dan transparansi penyimpanan data medis pasien dapat dikembangkan dengan menitikberatkan pada peningkatan interoperabilitas antar lembaga kesehatan. Fokus pengembangan dapat diarahkan pada standar protokol berbasis *blockchain* yang mampu terintegrasi dengan sistem *Electronic Health Record* (EHR) lintas rumah sakit, laboratorium, serta penyedia layanan asuransi kesehatan. Selain itu, penelitian lanjutan juga berpotensi mengeksplorasi pemanfaatan *Decentralized Identity* (DID) guna memperkuat autentikasi pengguna, serta memperluas fungsi smart contract agar dapat mengatur hak akses secara dinamis dan kontekstual, terutama dalam kondisi klinis atau situasi darurat (Ramadahni, 2024).

Di sisi lain, studi berikutnya dapat difokuskan pada analisis efisiensi dan skalabilitas jaringan *blockchain* dalam penerapannya di tingkat nasional serta model governance berbasis konsorsium, untuk menilai kemampuan sistem dalam menangani volume data medis yang besar tanpa mengorbankan kecepatan maupun privasi pengguna (Akhir et al., 2025).

Selain aspek teknis dan tata kelola, penelitian mendatang sebaiknya juga menekankan integrasi dengan Internet of Medical Things (IoMT) untuk memungkinkan data sensor medis real-time masuk ke *blockchain*, penerapan algoritma hemat energi seperti Proof-of-Stake, dan algoritma keamanan berbasis AI juga penting untuk mendukung sistem yang hemat energi, aman, dan sesuai dengan UU PDP.

KESIMPULAN

Penerapan teknologi *blockchain* dalam penyimpanan data medis menghadirkan solusi efektif terhadap isu keamanan, transparansi, dan efisiensi pengelolaan data pasien. Melalui karakteristik desentralisasi, *immutability*, dan *smart contract*, sistem ini memungkinkan pertukaran informasi medis yang aman dan dapat diaudit antar lembaga tanpa ketergantungan pada otoritas tunggal.

Secara teknis, arsitektur *hybrid on-chain* dan *off-chain* menjaga keseimbangan antara efisiensi dan keamanan, sementara enkripsi asimetris serta kontrol akses berbasis smart contract memperkuat perlindungan data. Penggunaan *permissioned blockchain* seperti *Hyperledger Fabric* memungkinkan pengaturan hak akses yang terukur, mendukung kolaborasi transparan antar rumah sakit, laboratorium, dan lembaga asuransi.

Secara ilmiah, *blockchain* menawarkan paradigma baru dalam tata kelola data medis melalui efisiensi proses administratif, optimalisasi rantai informasi, dan peningkatan keandalan audit digital. Dengan dukungan kebijakan yang adaptif, infrastruktur digital yang kuat, dan peningkatan kompetensi SDM, *blockchain* berpotensi menjadi fondasi transformasi digital sektor kesehatan Indonesia yang aman, terintegrasi, dan berkelanjutan. Namun, tantangan seperti skalabilitas, biaya, dan kepastian hukum tetap memerlukan riset lanjutan serta kolaborasi lintas sektor.



DAFTAR PUSTAKA

- Abdelsalam, F. M. (2023). Blockchain Revolutionizing Healthcare Industry: A Systematic Review of Blockchain Technology Benefits and Threats. *PubMed Central (PMC)*. Retrieved from <https://pmc.ncbi.nlm.nih.gov/articles/PMC10701638/>
- Akhir, N., Pertama, P., Kedua, P., Penulis, D., Artikel, K.-J., Pratiwi, I., & Widodo, S. (2025). Peran Teknologi Blockchain Terhadap Keamanan Dan Privasi Data Sistem Informasi Layanan Kesehatan: Studi Pustaka. *Indexia: Informatic and Computational Intelligent Journal*, 07(01), 11–18.
- Alexander, N., Wijaya, B. A., & Dewantoro, R. W. (2025). Penerapan Blockchain Untuk Keamanan Data Rekam Medis Elektronik: Literatur Review. *AT-TAKLIM: Jurnal Pendidikan Multidisiplin*, 2(3), 191–201.
- Ali, A., Ali, H., Saeed, A., Ahmed Khan, A., Tin, T. T., Assam, M., Ghadi, Y. Y., & Mohamed, H. G. (2023). Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning. *PubMed Central (PMC)*, 23(18), 7740. doi: 10.3390/s23187740
- Hamidah, U. F., & Pramono, P. (2024). Evaluasi Literatur Penggunaan Teknologi Blockchain dalam Sistem Terdistribusi untuk Pelayanan Kesehatan. *Prosiding Seminar Nasional Teknologi Informasi Dan Bisnis*, 574–578.
- HIPAA. (n.d.). *The HIPAA Privacy Rule*. Retrieved from <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>
- J, A., Isravel, D. P., Sagayam, K. M., Bhushan, B., Sei, Y., & Eunice, J. (2023). Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. In *Journal of Network and Computer Applications* (Vol. 215). Academic Press. doi: 10.1016/j.jnca.2023.103633
- Javan, R., Mohammadi, M., Beheshti-Atashgah, M., & Aref, M. R. (2024). *A Scalable Multi-Layered Blockchain Architecture for Enhanced EHR Sharing and Drug Supply Chain Management*. Retrieved from <http://arxiv.org/abs/2402.17342>
- Kamaruddin, I., Kraugusteliana, K., Surya, S., Musiana, M., & Tawil, M. R. (2024). Masalah kesehatan dan data dalam teknologi blockchain. *Jurnal Ners*, 8(1), 847–853.
- Lincopinis, D. R., & Llantos, O. E. (2024). The current research status of solving blockchain scalability issue. *Procedia Computer Science*, 239, 314–321. doi: 10.1016/j.procs.2024.06.177
- Mohammadi, M., Javan, R., Beheshti-Atashgah, M., & Aref, M. R. (2024). SCALHEALTH: Scalable Blockchain Integration for Secure IoT Healthcare Systems. *Cornell University*. Retrieved from



<https://arxiv.org/abs/2403.08068#:~:text=In%20this%20study%2C%20we%20introduce%20%28SCALHEALTH%29%20which%20is,confidentially.%20Also%2C%20sending%20data%20through%20IPFS%20is%20decentralized.>

Mohammed, R., Elmajid, E. A., Amine, H., & Khadija, C. (2023). Acceptance factors of telemedicine technology during Covid-19 pandemic among health professionals: A qualitative study. In *Healthcare Technology Letters* (Vol. 10, Issues 1–2, pp. 23–33). John Wiley and Sons Inc. doi: 10.1049/htl2.12042

Othman, S. Ben, & Getahun, M. (2025). Leveraging blockchain and IoMT for secure and interoperable electronic health records. *Scientific Reports*, 15(1), 12358. doi: 10.1038/s41598-025-95531-8

Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis, Pub. L. No. 24, Database Peraturan JDIH BPK (2022). Retrieved from <https://peraturan.bpk.go.id/Details/245544/permenkes-no-24-tahun-2022>

Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Pub. L. No. 27, Lembaran Negara Republik Indonesia (2022).

Pratiwi, I., & Widodo, S. (2025). Peran Teknologi Blockchain Terhadap Keamanan Dan Privasi Data Sistem Informasi Layanan Kesehatan: Studi Pustaka. *Indexia: Informatic and Computational Intelligent Journal*, 7(1), 11. doi: 10.30587/indexia.v7i1.9630

Ramadahni, K. (2024). Penerapan Teknologi Blockchain dalam Sistem Manajemen Kesehatan Elektronik. *Jurnal Sosial Teknologi*, 4(2), 116–119. doi: 10.59188/jurnalsostech.v4i2.1097

Samantray, B. S., & Reddy, K. H. K. (2025). A Federated Learning Approach Towards Hybrid Blockchain, Quantum-Key-Encryption based Distributed System: A Futuristic Healthcare Architecture for Smart Cities. *Blockchain: Research and Applications*, 100385. doi: 10.1016/j.bcra.2025.100385

Singh, M. K., Pippal, S. K., & Sharma, V. (2025). Lightweight blockchain mechanism for secure data transmission in healthcare system. *Biomedical Signal Processing and Control*, 102, 107411. doi: <https://doi.org/10.1016/j.bspc.2024.107411>

SIP Law Firm. (2025, July 14). *Keunggulan Teknologi Blockchain dan Relevansinya dalam Rekam Medis*. SIP Law Firm. Retrieved from <https://siplawfirm.id/keunggulan-teknologi-blockchain-dan-relevansinya-dalam-rekam-medis/?lang=id>

Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, 2(1), 55–68.



- Syukurillah, A. S., & Purwono, P. (2024). Penggunaan Blockchain dalam Rekam Medis Elektronik: Tinjauan Literatur Sistematis. *Jurnal Kolaborasi Riset Sarjana*, 1(1), 33–55.
- Tampubolon, J. O. Y., Bhawiyuga, A., & Siregar, R. A. (2022). Implementasi blockchain berbasis BigchainDB untuk menjamin keamanan data dalam sistem pencatatan rekam medis. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, 6(3), 1471–1480.
- Tawfik, A. M., Al-Ahwal, A., Eldien, A. S. T., & Zayed, H. H. (2025a). ACHealthChain blockchain framework for access control and privacy preservation in healthcare. *Scientific Reports*, 15(1). doi: 10.1038/s41598-025-00757-1
- Tawfik, A. M., Al-Ahwal, A., Eldien, A. S. T., & Zayed, H. H. (2025b). Blockchain-based access control and privacy preservation in healthcare: a comprehensive survey. *Cluster Computing*, 28(8), 529. doi: 10.1007/s10586-025-05308-x
- Wikarsa, L., Suwanto, T., & Lengkey, C. (2022). Implementasi Algoritma Konsensus Proof-of-Work dalam Blockchain terhadap Rekam Medis. *Jurnal Pekommas*, 7(1), 41–52. doi: 10.56873/jpkm.v7i1.4403