Vol. 7, No. 1, April 2026, hal. 112-120

Jurnal Computer Science and Information Technology (CoSciTech)

p-ISSN: 2723-567X
e-ISSN: 2723-5661

http://ejurnal.umri.ac.id/index.php/coscitech/index

Implementasi blockchain dalam keamanan data medis: tinjauan sistematis publish or perish

Salma Nasira Rusdha[1], Fauzan Ali Rahman[2] , Zelly Salmiyanti Rahman Zam[3], Vidi Prima Mizan[4], Fathihanna Yusuf[5] , Rahmi Oktarina[6]
Email: [1]salmanasira@student.unp.ac.id, [2]fauzanalirahman52@gmail.com,[3]zelly.salmi@gmail.com, [4]v.prima.mizan@gmail.com, [5]fathihannayusuf@gmail.com, [6]rahmi.oktarina@fpp.unp.ac.id

[12345]Departemen Kedokteran, Fakultas Kedokteran, Universitas Negeri Padang
[6]Departemen Ilmu Kesejahteraan Keluarga, Fakultas Pariwisata dan Perhotelan, Universitas Negeri Padang

Diterima: 7 Januari 2026 | Direvisi: 21 Februari 2026 | Disetujui: 27 April 2026

Abstrak

Digitalisasi layanan kesehatan menghadirkan peluang besar untuk meningkatkan efisiensi dan kualitas pelayanan, tetapi juga menimbulkan tantangan serius terkait keamanan, privasi, dan integritas data medis. Literatur menunjukkan bahwa sistem *Electronic Health Records* (EHR) konvensional masih rentan terhadap kebocoran data, manipulasi informasi, serta kegagalan sistem akibat arsitektur terpusat. Tinjauan ini menganalisis perkembangan teknologi *blockchain* sebagai solusi potensial dalam pengelolaan data kesehatan modern. Metode penelitian yang digunakan adalah tinjauan literatur sistematis dengan pendekatan *Publish or Perish*, menggunakan basis data Google Scholar untuk mengidentifikasi artikel ilmiah yang relevan, yang kemudian diseleksi berdasarkan kriteria inklusi dan eksklusi serta dianalisis secara kualitatif. Dengan karakteristik desentralisasi, *immutability*, kriptografi kuat, serta penggunaan *smart contract* untuk kontrol akses, blockchain menawarkan peningkatan signifikan terhadap keamanan, transparansi, dan interoperabilitas data medis. Penerapannya terlihat pada EHR, *telemedicine*, rantai pasok obat, citra medis, hingga pengelolaan data uji klinis. Namun, berbagai keterbatasan masih menghambat adopsi luas, termasuk masalah skalabilitas, beban komputasi, kompleksitas integrasi dengan sistem lama, dilema transparansi vs privasi, serta tantangan regulasi seperti kepatuhan terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP) dan standar internasional. Tren penelitian masa depan mengarah pada integrasi blockchain dengan AI, IoMT, dan *federated learning*, termasuk pengembangan *lightweight blockchain* untuk lingkungan dengan sumber daya terbatas. Secara keseluruhan, *blockchain* memiliki potensi besar dalam memperkuat keamanan dan keandalan sistem informasi kesehatan, tetapi implementasinya memerlukan pendekatan bertahap, terstandarisasi, dan sesuai regulasi.

Kata kunci: *blockchain, rekam medis elektronik, keamanan data medis, privasi data, interoperabilitas*.

Implementation of blockchain in medical data security: a systematic review of publish or perish

Abstract

The digitalization of healthcare services offers substantial opportunities to improve efficiency and quality of care; however, it also introduces significant challenges related to the security, privacy, and integrity of medical data. The literature indicates that conventional Electronic Health Record (EHR) systems remain vulnerable to data breaches, information manipulation, and system failures due to their centralized architecture. This review examines the development of blockchain technology as a potential solution for modern healthcare data management. The study employs a systematic literature review using the Publish or Perish approach, with Google Scholar as the data source to identify relevant scientific articles, which were subsequently screened based on predefined inclusion and exclusion criteria and analyzed qualitatively. Owing to its characteristics of decentralization, immutability, strong cryptography, and the use of smart contracts for access control, blockchain offers significant improvements in medical data security, transparency, and interoperability. Its applications have been reported in EHR systems, telemedicine, pharmaceutical supply chains, medical imaging, and clinical trial data management. Nevertheless, several limitations continue to hinder widespread adoption, including scalability issues, computational overhead, integration complexity with legacy systems, the transparency–privacy trade-off, and regulatory challenges such as compliance with data

protection laws and international standards. Future research trends point toward the integration of blockchain with artificial intelligence, the Internet of Medical Things (IoMT), and federated learning, as well as the development of lightweight blockchain solutions for resource-constrained environments. Overall, blockchain demonstrates considerable potential to strengthen the security and reliability of healthcare information systems; however, its implementation requires a gradual, standardized, and regulation-compliant approach.

Keywords: *blockchain, electronic health records, medical data security, privacy, interoperability*

1. PENDAHULUAN

Digitalisasi layanan kesehatan menuntut hadirnya sistem pengelolaan data yang aman, terintegrasi, dan mampu mendukung keputusan klinis secara efisien. *Electronic Health Records* (EHR) telah menjadi fondasi penting dalam modernisasi layanan kesehatan, tetapi implementasinya masih menghadapi berbagai permasalahan fundamental. Tantangan utama yang banyak ditemukan meliputi rendahnya interoperabilitas antar fasilitas layanan kesehatan, risiko kebocoran data, dan lemahnya mekanisme kontrol akses yang dapat mengancam privasi pasien [1]. Selain itu, sistem EHR konvensional yang bergantung pada server terpusat menjadikan data rentan terhadap serangan siber serta kegagalan sistem, sehingga dibutuhkan alternatif teknologi yang lebih aman dan berketahanan tinggi.

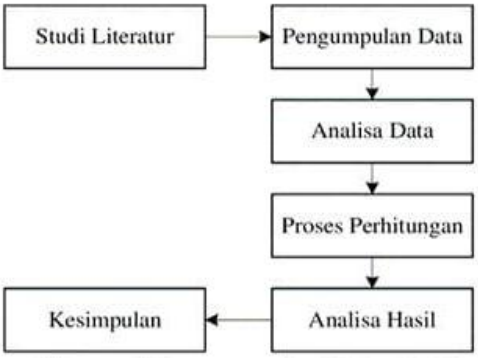
Teknologi *blockchain* muncul sebagai salah satu teknologi yang menawarkan solusi inovatif terhadap permasalahan tersebut. Sebagai *distributed ledger* yang bersifat *immutable*, transparan, dan terdesentralisasi, *blockchain* memungkinkan setiap transaksi data diverifikasi oleh banyak node sehingga meminimalkan potensi manipulasi data [2]. Dengan mekanisme kriptografi, *hashing*, dan *smart contracts*, *blockchain* tidak hanya meningkatkan integritas data, tetapi juga mampu mengatur hak akses secara otomatis dan memastikan jejak audit yang akurat. Dalam konteks kesehatan, karakteristik ini sangat relevan untuk memastikan keamanan data medis, validitas rekam medis, serta transparansi rantai pasok layanan dan obat.

Tinjauan literatur menunjukkan bahwa *blockchain* memiliki potensi besar untuk memperbaiki kualitas pengelolaan data kesehatan. Studi melaporkan bahwa integrasi *blockchain* dengan EHR dapat meningkatkan privasi dan interoperabilitas melalui pengaturan izin akses berbasis *smart contracts* [1]. Sementara itu, studi lain menegaskan bahwa *blockchain* mampu memperkuat keamanan, meningkatkan efisiensi proses digital, dan mendukung kolaborasi berbagai pihak melalui sistem pencatatan data yang tidak dapat diubah [2]. Selain itu, terdapat studi yang menunjukkan bahwa *blockchain* efektif mencegah manipulasi data dan melindungi privasi pengguna ketika diintegrasikan dengan teknologi seperti *edge computing* dan *federated learning* [3]. Namun demikian, literatur juga menyoroti sejumlah tantangan seperti skalabilitas, beban komputasi, kerumitan regulasi, dan kesiapan infrastruktur yang masih menjadi hambatan utama implementasi *blockchain* dalam sektor kesehatan [1], [3].

Berdasarkan kondisi tersebut, diperlukan kajian literatur sistematis untuk mengidentifikasi bagaimana *blockchain* dapat menjawab tantangan keamanan, privasi, dan interoperabilitas dalam sistem informasi kesehatan. Penelitian ini dilakukan untuk menganalisis perkembangan konsep *blockchain* dalam layanan kesehatan, mengevaluasi manfaat dan keterbatasannya, serta memetakan isu-isu yang masih menjadi hambatan implementasi. Dengan demikian, penelitian ini berupaya menjawab pertanyaan: *bagaimana implementasi blockchain dalam meningkatkan keamanan dan keandalan sistem informasi kesehatan, serta tantangan apa saja yang masih dihadapi dalam penerapannya?* Temuan dari kajian ini diharapkan dapat memberikan landasan konseptual yang kuat bagi penelitian lanjutan serta pengembangan sistem kesehatan berbasis *blockchain*.

2. METODE PENELITIAN

Penelitian ini menggunakan desain Tinjauan Literatur (*Literature Review*) dengan pendekatan kualitatif dan deskriptif-analitis untuk mengkaji peran teknologi blockchain dalam meningkatkan keamanan dan integritas data medis. Pencarian literatur dilakukan secara sistematis menggunakan perangkat lunak Publish or Perish dengan kueri "*Blockchain*" AND ("*Electronic Health Records*" OR "*Medical Records Systems*, *Computerized*" OR "*Health Information Systems*" OR "*Medical Data Security*" OR "*Patient Data Protection*"), dengan pemanfaatan operator Boolean AND dan OR untuk mempersempit fokus pencarian pada isu keamanan data medis berbasis *blockchain*. Literatur dibatasi pada publikasi ilmiah periode 2019–2025 yang bersumber dari jurnal dan prosiding bereputasi. Dari hasil penelusuran awal diperoleh 200 artikel dari *database* Google Scholar dan PubMed, yang selanjutnya diseleksi berdasarkan relevansi judul dan abstrak sehingga diperoleh 47 artikel dan referensi ilmiah untuk dianalisis lebih mendalam. Analisis data dilakukan melalui sintesis naratif dan analisis tematik, dengan tahapan pembacaan kritis dan ekstraksi data untuk mengidentifikasi tema-tema utama, meliputi kerentanan sistem *Electronic Health Records* (EHR) konvensional, mekanisme keamanan *blockchain* seperti desentralisasi, *immutability*, dan *smart contract*, serta ragam penerapannya dalam EHR, *telemedicine*, rantai pasok obat, pengelolaan citra medis, dan data uji klinis. Selain itu, kajian ini mengevaluasi mekanisme teknis *blockchain* yang mendukung keamanan data, termasuk kriptografi, enkripsi asimetris, dan mekanisme konsensus, serta mengidentifikasi tantangan implementasi krusial seperti isu skalabilitas, dilema privasi dan transparansi, integrasi dengan sistem yang telah ada, dan kepatuhan terhadap kerangka regulasi perlindungan data, termasuk HIPAA, GDPR, dan Undang-Undang Perlindungan Data Pribadi (UU PDP).



Gambar 1. Alur Proses Penelitian dalam *Literature Review*

3. HASIL DAN PEMBAHASAN

3.1. Konsep Dasar *Blockchain*

Teknologi *blockchain* merupakan suatu sistem pencatatan terdistribusi yang dirancang untuk menyimpan data dalam bentuk rangkaian blok yang saling terhubung melalui algoritme kriptografi [1]. Sifat desentralisasi, transparansi proses verifikasi, serta ketahanan terhadap modifikasi tidak sah menjadikan *blockchain* dipandang sebagai mekanisme yang mampu menjaga integritas dan autentisitas informasi, terutama pada data yang bersifat sensitif seperti rekam medis [4].

Struktur dasar *blockchain* tersusun atas beberapa komponen utama. Blok berperan sebagai unit data yang memuat transaksi yang telah divalidasi. Setiap blok diberi *hash*, yaitu nilai kriptografis yang menjadi identitas unik sekaligus penghubung dengan blok sebelumnya. *Smart contract* merupakan program otomatis yang menjalankan aturan tertentu dalam jaringan sehingga dapat mengatur alur akses atau pertukaran data tanpa intervensi manual. *Node* adalah perangkat yang menjalankan protokol jaringan, menyimpan salinan *ledger*, dan berpartisipasi dalam proses verifikasi. Seluruh aktivitas transaksi terdokumentasi dalam *ledger* terdistribusi yang disimpan pada setiap *node*, sehingga kegagalan atau kompromi pada satu titik tidak menghilangkan keseluruhan catatan [1], [5].

3.2. Tantangan Keamanan Data Medis Saat Ini

Transformasi sistem layanan kesehatan dari pencatatan berbasis kertas menuju ekosistem digital berbasis EHR, IoMT, komputasi awan, serta analitik berbasis kecerdasan buatan telah meningkatkan efisiensi layanan, tetapi sekaligus memperluas permukaan serangan terhadap data medis [6]. Digitalisasi ini membuat sistem kesehatan menghadapi berbagai risiko keamanan yang semakin kompleks. Perkembangan ini juga meningkatkan tekanan terhadap institusi layanan kesehatan untuk mematuhi standar keamanan data yang semakin ketat, karena sistem digital modern menuntut perlindungan kriptografis dan kebijakan keamanan yang lebih matang sesuai rekomendasi literatur keamanan kesehatan digital [7], [8], [9].

Salah satu tantangan utama adalah tingginya kerentanan terhadap kebocoran data akibat arsitektur penyimpanan yang masih terpusat dan penerapan enkripsi yang belum memadai. Kondisi ini menyebabkan rekam medis rawan diakses secara ilegal maupun disalahgunakan oleh pihak internal maupun eksternal [6], [10]. Selain itu, integritas data sering tidak terjaga dengan baik karena ketiadaan mekanisme audit dan verifikasi kriptografis yang memadai, sehingga memungkinkan terjadinya manipulasi data tanpa jejak [6], [10].

Interoperabilitas yang lemah antarplatform kesehatan juga menjadi sumber kerentanan. Perbedaan standar data dan protokol membuat proses pertukaran informasi rentan terhadap gangguan dan penyadapan, serta menghambat koordinasi layanan antarinstansi [6]. Di sisi lain, meningkatnya penggunaan perangkat IoMT memperluas titik serangan baru karena banyak perangkat memiliki kapasitas komputasi terbatas dan tidak mampu menerapkan protokol keamanan yang kuat [10].

Migrasi data kesehatan ke platform *cloud* meningkatkan tantangan keamanan yang semakin kompleks, termasuk risiko kebocoran informasi, kegagalan menjaga integritas data, konfigurasi yang tidak tepat, serta kerentanan pada mekanisme berbagi dan deduplikasi data. Infrastruktur kesehatan yang masih mengandalkan sistem lama juga tidak mampu menghadapi ancaman siber modern, sehingga institusi layanan kesehatan semakin rentan terhadap insiden seperti ransomware, serangan DDoS, maupun pencurian kredensial yang dapat mengganggu kontinuitas operasional. Temuan ini sejalan dengan kajian terbaru mengenai keamanan EMR berbasis *cloud* yang menekankan perlunya enkripsi lanjutan, kontrol akses yang ketat, audit penyimpanan, serta mekanisme perlindungan privasi untuk menjaga keamanan data pasien di lingkungan *cloud* [6], [7], [11], [12].

Kelemahan lainnya terletak pada kontrol akses yang belum granular, hak akses sering terlalu luas dan tidak memberikan kendali bagi pasien terhadap datanya sendiri. Minimnya transparansi dan jejak audit dalam pengelolaan data semakin menurunkan kepercayaan antar pemangku kepentingan karena sulit menelusuri asal-usul maupun perubahan data secara akurat [6],[10]. Di sisi lain, regulasi internasional seperti *Health Insurance Portability* and *Accountability Act* (HIPAA) dan General *Data Protection Regulation* (GDPR) serta kebijakan nasional mengenai perlindungan data pribadi menuntut penyedia layanan kesehatan untuk memastikan kerahasiaan integritas dan ketersediaan data. Kegagalan memenuhi standar ini meningkatkan risiko pelanggaran hukum dan etika dalam pengelolaan informasi kesehatan [13], [14].

3.3. Penerapan *Blockchain* dalam Bidang Kesehatan

Sektor kesehatan merupakan bidang yang bergantung secara intensif pada pengolahan data sensitif dari berbagai layanan, sehingga membutuhkan standar tinggi dalam aspek keamanan, kerahasiaan, serta interoperabilitas. Seluruh proses yang melibatkan akses data seperti penyimpanan, pertukaran, dan pembagian informasi harus berjalan secara aman dan terkontrol. Dalam konteks transformasi kesehatan digital, *Electronic Health Records* (EHR) menjadi komponen fundamental karena berfungsi sebagai media komunikasi *real time*, penyimpanan informasi medis, dan pengelolaan data secara terstruktur sesuai kebutuhan pengguna [15], [16].

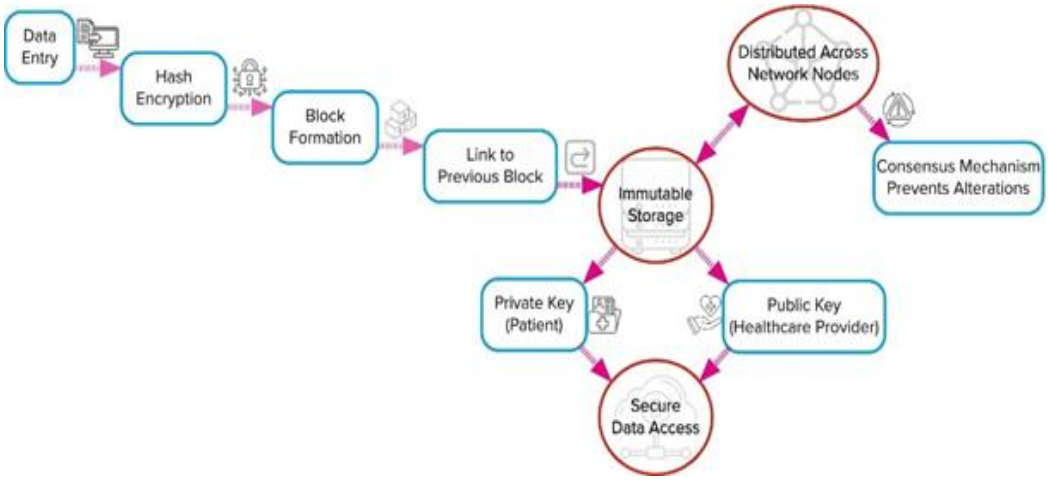
Seiring berkembangnya ekosistem kesehatan digital, sistem EHR semakin terintegrasi dengan teknologi pendukung seperti *Internet of Things* (IoT) dan algoritma *machine learning* untuk meningkatkan efisiensi layanan, pemantauan *real time*, dan dukungan pengambilan keputusan [17], [18]. Namun, penerapan teknologi tersebut meningkatkan kompleksitas pengelolaan data, khususnya terkait keamanan, integritas, dan kontrol akses data. Kondisi ini menegaskan kebutuhan akan arsitektur sistem informasi yang aman, terdistribusi, dan tepercaya dalam layanan kesehatan yang mengelola data sensitif pasien.

Dalam menjawab tantangan tersebut, pemanfaatan teknologi *blockchain* paling banyak dikembangkan pada sistem EHR. Teknologi *blockchain* memiliki karakteristik seperti *immutability*, desentralisasi, dan pencatatan transaksi yang transparan. Selain itu, penggunaan *smart contract* memungkinkan sistem kontrol akses yang lebih aman, dimana pasien dapat mengatur siapa saja yang berhak melihat atau menggunakan datanya [3], [19], [20]. Kemampuan *blockchain* dalam menjaga integritas data menjadi sangat relevan untuk pelayanan kesehatan yang bergantung pada pertukaran data dalam jumlah besar. Selain itu, kontrol akses, integritas, dan interoperabilitas menjadi aspek penting dalam memastikan data medis tetap terlindungi serta dapat dibagikan dengan aman antar fasilitas kesehatan [3], [20]. Selain pada rekam medis, penerapan *blockchain* juga berkembang pada berbagai layanan lain, terutama *telemedicine* yang semakin banyak digunakan pasca pandemi. Dalam *telemedicine*, *blockchain* berperan penting dalam memperkuat keamanan data dengan menyediakan mekanisme enkripsi terdesentralisasi dan pencatatan akses yang tidak dapat diubah, sehingga melindungi komunikasi antara pasien dokter dari potensi penyadapan serta kebocoran data selama proses konsultasi daring [21].

Di bidang farmasi, *blockchain* digunakan dalam rantai pasokan obat untuk memastikan keaslian produk dan mencegah peredaran obat palsu. Dengan *ledger* terdistribusi, setiap tahap distribusi obat dimulai dari produsen, distributor, hingga apotek dapat dilacak secara *real time* sehingga meningkatkan transparansi dan mendukung kepatuhan terhadap regulasi keamanan obat[22]. Sistem ini telah terbukti mampu mengurangi risiko pemalsuan dan mempercepat audit distribusi farmasi [23].

Pada pengelolaan citra medis seperti CT-scan dan MRI, *blockchain* membantu menjaga integritas file melalui penyimpanan *hash* digital yang menjamin citra tidak mengalami perubahan tanpa izin. Teknologi ini memungkinkan autentikasi citra medis secara otomatis, serta mempermudah pertukaran data antar rumah sakit tanpa mengurangi keamanan atau kualitas gambar [24], [25]. Di sisi lain, ukuran citra medis yang besar diatasi dengan model *off-chain storage*, sementara *blockchain* digunakan sebagai mekanisme audit dan verifikasi [26].

3.4. Mekanisme Keamanan Data dalam *Blockchain*



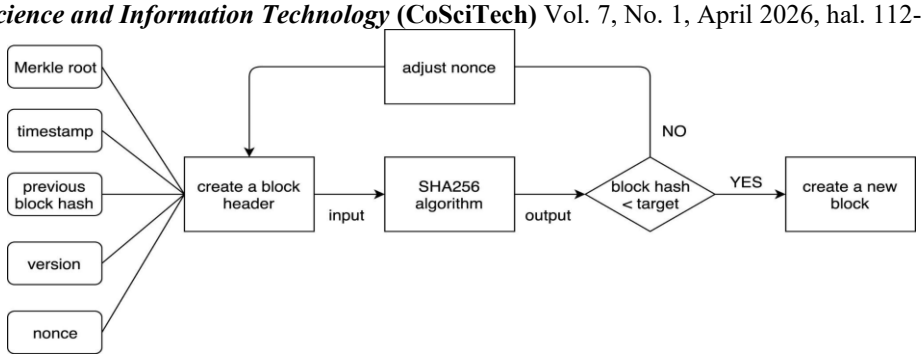
Gambar 2. Mekanisme Keamanan Data dalam *Blockchain* [27]

Mekanisme keamanan dalam *blockchain* dalam bidang medis bertumpu pada struktur jaringan yang terdesentralisasi dan bersifat *immutable*. Desentralisasi menghilangkan ketergantungan pada server tunggal (*single point of failure*), sehingga data kesehatan tersimpan pada banyak *node* dan jauh lebih sulit diretas atau dimanipulasi. Sifat *immutable* memastikan setiap transaksi yang telah tercatat tidak dapat diubah tanpa konsensus seluruh jaringan, sehingga integritas dan keaslian data tetap terjaga [27]. Lapisan keamanan ini diperkuat oleh penggunaan kriptografi modern, termasuk hashing dan enkripsi kunci publik-privat, yang berfungsi mengamankan kerahasiaan serta memastikan hanya pihak berotorisasi yang dapat mengakses data medis. Selain itu, *private key management* menjaga autentikasi pengguna, sementara *smart contract* mengatur izin akses secara otomatis berdasarkan protokol yang telah dirancang. Kombinasi mekanisme tersebut menciptakan sistem yang transparan, terlacak, dan sangat sulit untuk dimodifikasi, sehingga menawarkan tingkat keamanan yang lebih tinggi dibandingkan sistem pencatatan medis tradisional [28], [29].

Arsitektur *blockchain* yang terdesentralisasi menuntut penggunaan kriptografi dan enkripsi sebagai komponen utama keamanannya [30]. Kriptografi didefinisikan sebagai teknik yang mengubah data menjadi berbeda dari aslinya dengan menggunakan algoritme matematika sehingga orang yang tidak mengetahui kuncinya tidak akan dapat membongkar data tersebut [31]. Adapun, enkripsi didefinisikan sebagai tulisan dalam kode, sandi [32].

Sistem keamanan *blockchain* umumnya menggunakan enkripsi asimetris yang memanfaatkan sepasang kunci kriptografi, yaitu kunci publik dan kunci privat. Kedua kunci tersebut bekerja sebagai satu kesatuan yang memungkinkan proses enkripsi dan dekripsi dilakukan secara terpisah namun tetap saling terkait. Kunci privat dibangkitkan melalui algoritma pembangkitan kunci yang menghasilkan nilai yang tidak dapat diprediksi, kemudian kunci publik dibentuk dari kunci privat melalui *one-way irreversible computation*, yaitu proses matematis satu arah yang tidak dapat dibalik. Pada mekanisme ini data dienkripsi menggunakan salah satu kunci dan hanya dapat didekripsi oleh kunci pasangannya, sehingga menjaga kerahasiaan dan autentikasi data. Sifat komputasi satu arah inilah yang memastikan bahwa data pada *blockchain* tetap aman meskipun ditransmisikan melalui jaringan internet publik [30], [33].

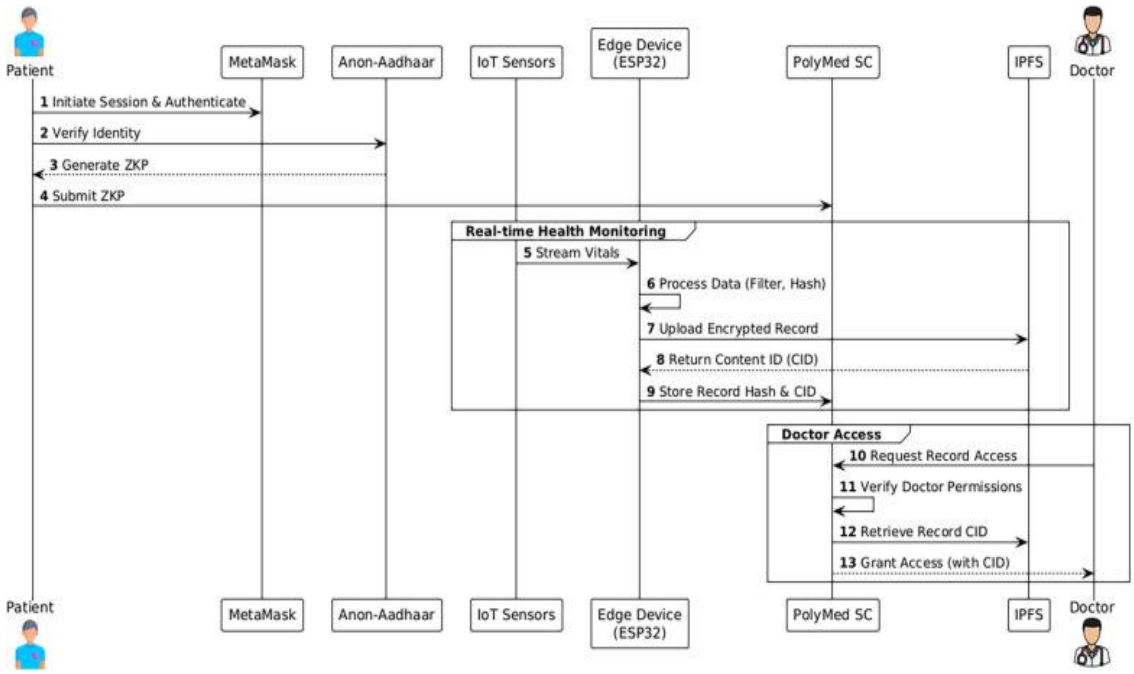
Untuk menjaga validitas data dalam sistem *blockchain* yang terdesentralisasi, diperlukan mekanisme konsensus. Dalam mekanisme ini, tidak mengizinkan kepemilikan otoritatif terhadap suatu data, memungkinkan setiap partisipan atau *node* dalam *blockchain* untuk sepakat atas validitas suatu data [30], [33], [31]. Terdapat beberapa algoritma yang digunakan dalam mekanisme konsensus diantaranya ialah algoritma *Proof of Work.* Algoritma ini menentukan salah satu *node* untuk bertanggung jawab dalam membentuk blok baru, penentuan ini dilakukan melalui sayembara, *node* yang mampu memecahkan *puzzle* kriptografi terlebih dahulu adalah *node* yang diberi wewenang untuk membentuk blok baru. Namun, mekanisme ini sangat bergantung pada kemampuan komputasi, karena setiap *puzzle* merupakan susunan kompleks yang tak bisa diprediksi. Selain itu, hal tersebut menyebabkan mekanisme ini aman, karena untuk membuat suatu rantai palsu dibutuhkan daya komputasi yang sangat besar [30], [33], [31].



Gambar 3. Algoritma *Proof of Work* dalam *Blockchain* [34]

3.5. Integrasi *Blockchain* dengan Teknologi Lain

Teknologi *blockchain* merupakan sistem pencatatan data yang secara inheren memiliki sifat desentralisasi, *immutability*, dan transparansi [30], [33], [31]. Sifat ini menjadikannya solusi potensial untuk meningkatkan keamanan dan integritas data dalam sistem kesehatan digital yang membutuhkan perlindungan data sensitif dan otomatisasi proses administratif. PolyMed menggabungkan *blockchain*, AI, dan IoMT untuk membangun *electronic health record* (EHR) berbasis *blockchain* yang terotomatisasi, mencakup autentikasi pengguna, penyimpanan rekam medis digital, penjadwalan otomatis, dan manajemen preskripsi. Integrasi AI dengan IoMT memungkinkan pemantauan tanda vital secara *real time*, deteksi anomali, kondisi emergensi, serta membantu pasien menjadwalkan konsultasi dengan klinisi [35]. Pendekatan ini menghadirkan sistem kesehatan digital yang aman, efisien, dan berfokus pada pasien, sekaligus memanfaatkan potensi penuh *blockchain* dan teknologi cerdas.



Gambar 4. Peranan Blockchain dalam PolyMed [35]

3.6. Tantangan dan Keterbatasan Implementasi

Implementasi *blockchain* untuk *Electronic Health Records* (EHR) menawarkan peningkatan keamanan, integritas, dan kendali pasien, tetapi literatur menekankan bahwa tantangan teknis dan regulatif masih signifikan. Masalah skalabilitas dan *latency* muncul karena keterbatasan *throughput* pada *platform* seperti Ethereum, ditambah pertumbuhan *ledg*er yang sangat cepat, sehingga meningkatkan beban penyimpanan dan komputasi pada seluruh *node* jaringan [36]. Solusi seperti penyimpanan *off-chain* menggunakan IPFS, penggunaan konsensus PBFT, serta arsitektur *sidechain* dikembangkan untuk mengurangi *bottleneck*, tetap menyisakan kompleksitas operasional dan potensi konsumsi energi tinggi [37].

Dilema utama adalah *trade-off* antara transparansi dan privasi. Sifat dasar *blockchain* yang transparan dan *immutable* sering bertentangan dengan regulasi privasi medis yang ketat. *Permissionless blockchain* dapat membuka risiko *deanonymization* melalui analisis metadata dan pola transaksi, sehingga tidak ideal untuk EHR [38]. Penerapan *framework* seperti *Healthchain*

yang menggunakan enkripsi berlapis (AES-256, RSA, ECC), *hash on-chain*, dan kontrol akses berbasis peran via *smart contracts*, tetap memiliki risiko kebocoran metadata [8]. Kendala lain yang dominan adalah interoperabilitas dengan sistem EHR lama yang silo dan beragam formatnya (HL7 v2, CDA, FHIR). Selain itu, integrasi model seperti MedRec, FHIRChain, dan Ancile tetap membutuhkan transformasi data, pemetaan semantik, serta sinkronisasi multi-sistem, ditambah penyesuaian *workflow* klinis, pelatihan tenaga kesehatan, dan ketergantungan pada vendor lama [39].

Dari aspek hukum dan etis, tantangan muncul dari konflik antara sifat *immutable blockchain* dan regulasi internasional seperti HIPAA dan GDPR, termasuk hak untuk menghapus data (*right to be forgotten*) dan prinsip *data minimization*. Di Indonesia, regulasi UU PDP No. 27/2022 dan Permenkes No. 24/2022 menuntut kontrol data berada pada fasilitas pelayanan kesehatan, sementara *blockchain* mendistribusikan otoritas secara desentralisasi [40], [41]. *Hybrid encryption* dan *sidechain* membantu mendekati kepatuhan, tetapi isu tanggung jawab hukum dan akses tetap menjadi penghalang adopsi luas [37].

3.7. Tren dan Arah Penelitian Masa Depan

Arah penelitian masa depan dalam ekosistem kesehatan digital terdesentralisasi didorong oleh sinergi antara *Federated Learning* (FL) berbasis *Blockchain* (BCFL), yang bertujuan menciptakan kerangka kerja yang aman, terdesentralisasi, dan patuh terhadap regulasi. Tren utama adalah mengatasi tantangan yang melekat pada FL tradisional dengan mengintegrasikan *blockchain* untuk memberikan mekanisme insentif dan verifikasi integritas model yang lebih kuat, sekaligus memastikan transparansi dan kontrol penuh pasien atas data kesehatan mereka [42]. Dalam konteks ini, penelitian mendalam berfokus pada desain fitur kunci seperti protokol konsensus yang disesuaikan, protokol kriptografi, dan topologi penyimpanan, yang sangat relevan untuk kasus penggunaan kesehatan yang menuntut keamanan dan privasi tinggi [43]. Pengembangan BCFL terbukti signifikan dalam meningkatkan kepercayaan, verifikasi, dan auditabilitas dalam sistem FL kesehatan.

Meskipun demikian, adopsi teknologi ini diperumit oleh keterbatasan sumber daya komputasi dan energi pada Perangkat Medis (IoMT). Oleh karena itu, arah penelitian bergeser ke pengembangan *Lightweight Blockchain* yang spesifik untuk lingkungan IoMT yang *resource-constrained* [44]. Fokus utama adalah merancang protokol konsensus yang dioptimalkan dan hemat energi, seperti modifikasi *Proof-of-Authority* (PoA) atau *Delegated Proof of Stake* (DPoS), untuk mengurangi beban komputasi dan latensi yang tinggi [45], [46]. Pendekatan ini melibatkan pengalihan tugas validasi dan konsensus ke *edge nodes* atau *gateway*, melepaskan perangkat medis individual dari tuntutan pemrosesan yang berat, dan meningkatkan skalabilitas jaringan [44], [46].

Di samping tantangan teknis, keberhasilan implementasi BCFL secara global sangat bergantung pada Standardisasi Interoperabilitas Global dan Regulasi Kebijakan yang mendukung adopsi. Terdapat kebutuhan mendesak untuk mengembangkan skema data standar yang memungkinkan pertukaran *Electronic Health Records* (EHR) dan wawasan model secara mulus antar sistem *blockchain* yang berbeda. Lebih lanjut, kerangka kerja regulasi harus dirancang untuk secara inheren mematuhi persyaratan privasi data internasional, seperti HIPAA dan GDPR [43]. Di sini, penelitian berfokus pada pemanfaatan smart contract untuk mengotomatisasi dan menegakkan kebijakan kontrol akses secara granular, mencatat semua tindakan dalam buku besar yang transparan. Hal ini tidak hanya memastikan kepatuhan terhadap kebijakan yang ditetapkan, tetapi juga memfasilitasi audit yang mudah dan menyediakan catatan *immutable* tentang siapa yang mengakses data, sehingga memperkuat pertanggungjawaban dalam sistem kesehatan [47], [48], [49].

4. KESIMPULAN

Teknologi *blockchain* menawarkan pendekatan inovatif untuk keamanan data medis di era digital. Digitalisasi layanan kesehatan tidak hanya meningkatkan efisiensi dan efektivitas, tetapi juga membuka risiko kebocoran data sensitif yang dapat dimanfaatkan pihak tidak bertanggung jawab. *Blockchain* mengatasi tantangan ini melalui karakteristik desentralisasi, enkripsi, dan catatan yang tidak dapat diubah (*immutable ledger*) serta terikat pada *timestamp*, sehingga menjamin integritas, kerahasiaan, dan autentikasi data. Mekanisme *smart contract* memastikan akses data hanya diberikan kepada pihak berwenang, sementara kemampuan integrasi dengan teknologi lain seperti AI dan IoMT memungkinkan sistem medis lebih fleksibel, efisien, dan berorientasi pada pasien.

Meskipun demikian, implementasi *blockchain* memerlukan pertimbangan matang terkait skalabilitas, latensi, biaya komputasi, keseimbangan antara privasi dan transparansi, integrasi dengan sistem EHR lama, serta aspek etis dan regulasi. Keberhasilan adopsi *blockchain* bergantung pada strategi yang terstruktur, kolaborasi lintas pemangku kepentingan, dan kesadaran kolektif. Dengan penerapan yang tepat, *blockchain* berpotensi dalam transformasi keamanan data medis, membangun sistem kesehatan yang aman, inklusif, dan demokratis, serta meningkatkan kepercayaan pasien terhadap layanan digital.

Ucapan Terima kasih

Penulis mengucapkan terima kasih kepada Fakultas Kedokteran Universitas Negeri Padang atas dukungan fasilitas penelitian dan akses literatur selama penyusunan kajian ini. Bantuan dan arahan dari staf pengajar serta pihak terkait lainnya, baik secara langsung maupun tidak langsung, sangat membantu sehingga penelitian ini dapat memberikan kontribusi bagi pengembangan ilmu kedokteran dan teknologi kesehatan.

DAFTAR PUSTAKA

[1] Y. Han, Y. Zhang, and S. H. Vermund, "Blockchain Technology for Electronic Health Records," *Int. J. Environ. Res. Public. Health*, vol. 19, no. 23, p. 15577, Nov. 2022, doi: 10.3390/ijerph192315577.

[2] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *Int. J. Intell. Netw.*, vol. 2, pp. 130–139, 2021, doi: 10.1016/j.ijin.2021.09.005.

[3] H. Taherdoost, "Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives," *Sci*, vol. 5, no. 4, p. 41, Oct. 2023, doi: 10.3390/sci5040041.

[4] A. Sharma, R. Chauhan, S. Gupta, and A. Kapruwan, "Blockchain revolution in healthcare: A comprehensive survey," in *Challenges in Information, Communication and Computing Technology*, 1st ed., London: CRC Press, 2024, pp. 218–223. doi: 10.1201/9781003559085-38.

[5] A. A. Monrat, O. Schelen, and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019, doi: 10.1109/ACCESS.2019.2936094.

[6] A. J, D. P. Isravel, K. M. Sagayam, B. Bhushan, Y. Sei, and J. Eunice, "Blockchain for healthcare systems: Architecture, security challenges, trends and future directions," *J. Netw. Comput. Appl.*, vol. 215, p. 103633, June 2023, doi: 10.1016/j.jnca.2023.103633.

[7] G. Liu, H. Xie, W. Wang, and H. Huang, "A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption," *J. Cloud Comput.*, vol. 13, no. 1, p. 44, Feb. 2024, doi: 10.1186/s13677-024-00608-w.

[8] K. Sabiri, F. Sousa, and T. Rocha, "A systematic review of privacy-preserving blockchain applications in healthcare," *Multimed. Tools Appl.*, vol. 84, no. 32, pp. 39925–39980, Mar. 2025, doi: 10.1007/s11042-024-20541-z.

[9] A. Alabdulatif, "Blockchain-Based Privacy-Preserving Authentication and Access Control Model for E-Health Users," *Information*, vol. 16, no. 3, p. 219, Mar. 2025, doi: 10.3390/info16030219.

[10] A. Corte-Real, T. Nunes, and P. R. Da Cunha, "Reflections about Blockchain in Health Data Sharing: Navigating a Disruptive Technology," *Int. J. Environ. Res. Public. Health*, vol. 21, no. 2, p. 230, Feb. 2024, doi: 10.3390/ijerph21020230.

[11] J. Yu, W. Shen, and X. Zhang, "Cloud storage auditing and data sharing with data deduplication and private information protection for cloud-based EMR," *Comput. Secur.*, vol. 144, p. 103932, Sept. 2024, doi: 10.1016/j.cose.2024.103932.

[12] H. Yi, "Improving cloud storage and privacy security for digital twin based medical records," *J. Cloud Comput.*, vol. 12, no. 1, p. 151, Oct. 2023, doi: 10.1186/s13677-023-00523-6.

[13] M. Jurczuk and M. Suprunowicz, "Consent in Data Privacy: A General Comparison of GDPR and HIPAA," *Przegląd Praw. Uniw. Im Adam Mickiewicza*, vol. 16, pp. 173–194, Dec. 2024, doi: 10.14746/ppuam.2024.16.07.

[14] S. Barbaria, A. Jemai, H. İ. Ceylan, R. I. Muntean, I. Dergaa, and H. Boussi Rahmouni, "Advancing Compliance with HIPAA and GDPR in Healthcare: A Blockchain-Based Strategy for Secure Data Exchange in Clinical Research Involving Private Health Information," *Healthcare*, vol. 13, no. 20, p. 2594, Oct. 2025, doi: 10.3390/healthcare13202594.

[15] A. L. A. Fonsêca *et al.*, "Blockchain in Health Information Systems: A Systematic Review," *Int. J. Environ. Res. Public. Health*, vol. 21, no. 11, p. 1512, Nov. 2024, doi: 10.3390/ijerph21111512.

[16] A. G. Chandini and P. I. Basarkod, "Patient centric pre-transaction signature verification assisted smart contract based blockchain for electronic healthcare records," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 4, pp. 4221–4235, Apr. 2023, doi: 10.1007/s12652-023-04526-8.

[17] D. F. Dava, K. Kamdan, and Z. Alamsyah, "Pemanfaatan Tongkat Berbasis IoT dan Yolo V3 Untuk Meningkatkan Mobilitas dan Keamanan Penyandang Tunanetra," *J. CoSciTech Comput. Sci. Inf. Technol.*, vol. 6, no. 2, pp. 94–103, Aug. 2025, doi: 10.37859/coscitech.v6i2.9793.

[18] P. Marchanda Izzati and F. Fitriyani, "Implementasi Algoritma XGBoost Untuk Prediksi Capaian Bulanan Pendapatan Daerah Kota Bandung," *J. CoSciTech Comput. Sci. Inf. Technol.*, vol. 6, no. 2, pp. 104–111, Aug. 2025, doi: 10.37859/coscitech.v6i2.9578.

[19] A. Agbeyangi, O. Oki, and A. Mgidi, "Blockchain in Healthcare: Implementing Hyperledger Fabric for Electronic Health Records at Frere Provincial Hospital," 2024, *arXiv*. doi: 10.48550/ARXIV.2407.15876.

[20] D. B. Santoso, A. Fuad, G. B. Herwanto, and A. W. Maula, "BLOCKCHAIN TECHNOLOGY IMPLEMENTATION ON MEDICAL RECORDS DATA MANAGEMENT: A REVIEW OF RECENT STUDIES," *J. Ris. Kesehat.*, vol. 9, no. 2, pp. 107–112, Nov. 2020, doi: 10.31983/jrk.v9i2.5742.

[21] X. Liang, N. Alam, T. Sultana, E. Bandara, and S. Shetty, "Designing A Blockchain-Empowered Telehealth Artifact for Decentralized Identity Management and Trustworthy Communication: Interdisciplinary Approach," *J. Med. Internet Res.*, vol. 26, p. e46556, Sept. 2024, doi: 10.2196/46556.

[22] W. Nova, "ANALISIS PENERAPAN TEKNOLOGI BLOCKCHAIN UNTUK MENINGKATKAN KEAMANAN DAN TRACEABILITY PADA RANTAI PASOK OBAT," 2025, doi: 10.13140/RG.2.2.32677.36327.

[23] V. Lingayat, I. Pardikar, S. Yewalekar, S. Khachane, and S. Pande, "Securing Pharmaceutical Supply Chain using Blockchain Technology," *ITM Web Conf.*, vol. 37, p. 01013, 2021, doi: 10.1051/itmconf/20213701013.

[24] A. S. Tagliafico *et al.*, "Blockchain in radiology research and clinical practice: current trends and future directions," *Radiol. Med. (Torino)*, vol. 127, no. 4, pp. 391–397, Apr. 2022, doi: 10.1007/s11547-022-01460-1.

[25] R. Kumar *et al.*, "An Integration of blockchain and AI for secure data sharing and detection of CT images for the hospitals," *Comput. Med. Imaging Graph.*, vol. 87, p. 101812, Jan. 2021, doi: 10.1016/j.compmedimag.2020.101812.

[26] J. Mythili and R. Gopalakrishnan, "Improving data transmission through optimizing blockchain sharding in cloud IoT based healthcare applications," *Egypt. Inform. J.*, vol. 30, p. 100661, June 2025, doi: 10.1016/j.eij.2025.100661.

[27] S. Felemban *et al.*, "Current application of blockchain technology in healthcare and its potential roles in Urology," *BJU Int.*, vol. 136, no. S2, Oct. 2025, doi: 10.1111/bju.16757.

[28] M. K. Singh, S. K. Pippal, and V. Sharma, "Lightweight blockchain mechanism for secure data transmission in healthcare system," *Biomed. Signal Process. Control*, vol. 102, p. 107411, Apr. 2025, doi: 10.1016/j.bspc.2024.107411.

[29] M. A. Al-Khasawneh, M. Faheem, A. A. Alarood, S. Habibullah, and A. Alzahrani, "A secure blockchain framework for healthcare records management systems," *Healthc. Technol. Lett.*, vol. 11, no. 6, pp. 461–470, Dec. 2024, doi: 10.1049/htl2.12092.

[30] L. Guo, H. Xie, and Y. Li, "Data encryption based blockchain and privacy preserving mechanisms towards big data," *J. Vis. Commun. Image Represent.*, vol. 70, p. 102741, July 2020, doi: 10.1016/j.jvcir.2019.102741.

[31] Kamus Besar Bahasa Indonesia, "Kriptografi," *KBBI*. in Edisi III. Badan Pengembangan dan Pembinaan Bahasa (Pusat Bahasa).

[32] Kamus Besar Bahasa Indonesia, "Enkripsi," *KBBI*. in Edisi III. Badan Pengembangan dan Pembinaan Bahasa (Pusat Bahasa).

[33] S. Zhai, Y. Yang, J. Li, C. Qiu, and J. Zhao, "Research on the Application of Cryptography on the Blockchain," *J. Phys. Conf. Ser.*, vol. 1168, p. 032077, Feb. 2019, doi: 10.1088/1742-6596/1168/3/032077.

[34] S. Zhang and J.-H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT Express*, vol. 6, no. 2, pp. 93–97, June 2020, doi: 10.1016/j.icte.2019.08.001.

[35] H. Kumar A., P. Venkatram C., S. N., D. Daniel, and P. Joe I. R., "Decentralized digital health ecosystems: a unified architecture for AI-enhanced medical record management," *Front. Digit. Health*, vol. 7, p. 1685628, Oct. 2025, doi: 10.3389/fdgth.2025.1685628.

[36] P. M. Katoon and A. V. Turukmane, "Interoperable blockchain network for healthcare data using Fabric, Ethereum and IPFS," *Discov. Artif. Intell.*, vol. 5, no. 1, p. 308, Nov. 2025, doi: 10.1007/s44163-025-00564-7.

[37] A. Alamsyah and I. P. S. Setiawan, "Enhancing privacy and traceability of public health insurance claim system using blockchain technology," *Front. Blockchain*, vol. 8, p. 1474434, Feb. 2025, doi: 10.3389/fbloc.2025.1474434.
[38] Y. Shynar *et al.*, "Comprehensive Analysis of Blockchain Technology in the Healthcare Sector and Its Security Implications:," *Int. J. E-Health Med. Commun.*, vol. 16, no. 1, pp. 1–45, Apr. 2025, doi: 10.4018/IJEHMC.372423.
[39] S. Schmeelk, M. Kanabar, K. Peterson, and J. Pathak, "Electronic health records and blockchain interoperability requirements: a scoping review," *JAMIA Open*, vol. 5, no. 3, p. ooac068, July 2022, doi: 10.1093/jamiaopen/ooac068.
[40] Indonesia, Pemerintah Pusat, "Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi." Badan Pembinaan dan Pengembangan Hukum Pemeriksaan Keuangan Negara Badan Pemeriksa Keuangan.
[41] Indonesia, Kementerian Kesehatan, "Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis." Badan Pembinaan dan Pengembangan Hukum Pemeriksaan Keuangan Negara Badan Pemeriksa Keuangan, Agustus 2022.
[42] D. C. Nguyen *et al.*, "Federated Learning for Smart Healthcare: A Survey," *ACM Comput. Surv.*, vol. 55, no. 3, pp. 1–37, Mar. 2023, doi: 10.1145/3501296.
[43] Y. Shahsavari, O. A. Dambri, Y. Baseri, A. S. Hafid, and D. Makrakis, "Integration of Federated Learning and Blockchain in Healthcare: A Tutorial," 2024, *arXiv*. doi: 10.48550/ARXIV.2404.10092.
[44] S. Sahraoui and A. Bachir, "Lightweight consensus mechanisms in the Internet of Blockchained Things: Thorough analysis and research directions," *Digit. Commun. Netw.*, vol. 11, no. 4, pp. 1246–1261, Aug. 2025, doi: 10.1016/j.dcan.2024.12.007.
[45] F. D. Tarzjani and M. Salehi, "An Efficient Lightweight Blockchain for Decentralized IoT," 2025, *arXiv*. doi: 10.48550/ARXIV.2508.19219.
[46] G. Maya, A. Sathiya, S. C. K, R. Hemalatha, S. Punitha, and M. Udhayamoorthi, "A Blockchain-based Lightweight Security Framework for IoT-Enabled Smart Healthcare Systems," in *2025 Third International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, Trichy, India: IEEE, May 2025, pp. 978–984. doi: 10.1109/ICAISS61471.2025.11041765.
[47] N. Yaqub *et al.*, "Blockchain enabled policy-based access control mechanism to restrict unauthorized access to electronic health records," *PeerJ Comput. Sci.*, vol. 11, p. e2647, Jan. 2025, doi: 10.7717/peerj-cs.2647.
[48] M. A. Amin, H. Tummala, S. Mohan, and I. Ray, "Healthcare Policy Compliance: A Blockchain Smart Contract-Based Approach," 2023, *arXiv*. doi: 10.48550/ARXIV.2312.10214.
[49] J. Habu, A. S. Dhabariya, B. L. Pal, and F. A. Abubakar, "Decentralized Data Governance and Regulatory Compliance in Federated Learning and Edge Computing for Healthcare," May 09, 2025, *In Review*. doi: 10.21203/rs.3.rs-6295183/v1.