PENERAPAN TEKNOLOGI BLOCKCHAIN DALAM PENGAMANAN DATA SISTEM INFORMASI

Abstrak

Perkembangan sistem informasi digital menyebabkan meningkatnya ancaman terhadap keamanan data di berbagai sektor, terutama pada sistem terpusat yang rawan terhadap serangan siber dan kegagalan sistem. Teknologi blockchain hadir sebagai solusi alternatif dengan prinsip desentralisasi, kriptografi canggih, dan mekanisme konsensus yang menjamin integritas serta keaslian data tanpa otoritas pusat. Penelitian ini bertujuan untuk menganalisis peran blockchain dalam meningkatkan keamanan data sistem informasi serta implementasinya di sektor publik Indonesia. Metode yang digunakan adalah pendekatan kualitatif deskriptif melalui studi literatur sistematis terhadap jurnal, laporan BSSN, dan regulasi nasional terkait keamanan data dan blockchain pada periode 2020–2025. Hasil penelitian menunjukkan bahwa penerapan blockchain mampu meningkatkan integritas dan ketahanan data hingga 90%, menghilangkan single point of failure, serta mendukung transparansi dan self-sovereign identity (SSI) bagi pengguna. Meskipun demikian, tantangan seperti skalabilitas, biaya awal, serta kesiapan regulasi masih menjadi kendala utama untuk adopsi luas. Secara keseluruhan, blockchain berpotensi besar memperkuat keamanan sistem informasi di Indonesia dan menjadi fondasi bagi penerapan trustless system di era digital.

Kata Kunci: Blockchain, Keamanan Data, Sistem Informasi

Abstract

The development of digital information systems has led to increasing threats to data security in various sectors, particularly centralized systems that are vulnerable to cyberattacks and system failures. Blockchain technology offers an alternative solution, based on the principles of decentralization, advanced cryptography, and consensus mechanisms that guarantee data integrity and authenticity without a central authority. This study aims to analyze the role of blockchain in improving information system data security and its implementation in the Indonesian public sector. The method used is a descriptive qualitative approach through a systematic literature review of journals, BSSN reports, and national regulations related to data security and blockchain for the 2020–2025 period. The results show that blockchain implementation can increase data integrity and resilience by up to 90%, eliminate single points of failure, and support transparency and self-sovereign identity (SSI) for users. However, challenges such as scalability, initial costs, and regulatory readiness remain major obstacles to widespread adoption. Overall, blockchain has significant potential to strengthen information system security in Indonesia and serve as a foundation for implementing trustless systems in the digital era.

Keywords: Blockchain, Data Security, Information Systems

PENDAHULUAN

Perkembangan sistem informasi telah merevolusi cara organisasi dan individu mengelola data di era digital saat ini. Dimulai dari era komputer pribadi pada 1980-an hingga transformasi digital melalui cloud computing, Internet of Things (IoT), kecerdasan buatan (AI), dan big data analytics, sistem informasi kini menjadi tulang punggung operasional global. Menurut data dari Badan Siber dan Sandi Negara (BSSN) Indonesia, volume data dunia diproyeksikan mencapai 181 zettabyte pada 2025, didorong oleh proliferasi perangkat terhubung yang melebihi 75 miliar unit. Namun, kemajuan ini disertai peningkatan ancaman keamanan data yang eksponensial. Serangan siber seperti phishing, ransomware, distributed denial-of-service (DDoS), dan advanced persistent threats (APT) melonjak tajam; misalnya, laporan BSSN mencatat peningkatan 22% insiden siber di Indonesia pada 2022 saja, dengan kerugian ekonomi mencapai triliunan rupiah. Faktor pendorong termasuk digitalisasi layanan publik, e-commerce, dan remote work pasca-pandemi, yang memperluas permukaan serangan (attack surface). Di Indonesia, kasus peretasan Pusat Data Nasional pada 2024 dan kebocoran data BPJS Kesehatan menunjukkan kerentanan infrastruktur nasional terhadap aktor negara dan kriminal siber. Ancaman ini tidak hanya mengancam privasi individu tetapi juga stabilitas ekonomi dan keamanan nasional, memaksa organisasi untuk terus beradaptasi (Wirawan, 2020).

Kelemahan utama sistem keamanan data konvensional terletak pada arsitektur sentralisasi dan konsep single point of failure (SPOF). Dalam model tradisional, data disimpan di server pusat atau database terpusat seperti SQL server di cloud provider tunggal (misalnya AWS atau Azure), di mana satu titik akses mengendalikan seluruh ekosistem. SPOF terjadi ketika kegagalan komponen kritis seperti server utama, firewall, atau oracle pihak ketiga menyebabkan kehancuran total sistem. Contoh nyata termasuk kebakaran Gedung Cyber 1 milik BSSN yang mengganggu layanan siber nasional atau serangan ransomware WannaCry 2017 yang melumpuhkan ribuan sistem global karena ketergantungan pada patch tunggal dari Microsoft (Raharjo et al., 2022). Sentralisasi ini rentan terhadap serangan brute force, man-in-the-middle (MitM), atau insider threats, di

mana peretas hanya perlu menembus satu lapisan pertahanan untuk mengakses semuanya. Selain itu, skalabilitas terbatas dan ketergantungan pada trusted third party (TTP) seperti certificate authorities meningkatkan risiko kompromi massal. Di konteks Indonesia, regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) 2022 menekankan kelemahan ini, karena sistem konvensional sulit memenuhi prinsip zero-trust architecture. Akibatnya, downtime bisa berlangsung berhari-hari, kehilangan data permanen, dan tuntutan hukum yang mahal, seperti yang dialami perusahaan telekomunikasi lokal akibat kebocoran 279 juta data pengguna pada 2021 (Sinaga & Harahap, 2020).

Blockchain muncul sebagai teknologi alternatif disruptif untuk mengatasi kelemahan tersebut melalui prinsip desentralisasi dan kriptografi canggih. Berbeda dengan database sentral, blockchain adalah ledger terdistribusi yang menyimpan data dalam blok-blok yang dihubungkan secara kriptografis dan direplikasi ke ribuan node independen di jaringan peer-to-peer (P2P). Setiap transaksi diverifikasi melalui mekanisme konsensus seperti Proof-of-Work (PoW) atau Proof-of-Stake (PoS), memastikan immutability data sekali ditulis tidak bisa diubah tanpa persetujuan mayoritas node. Ini menghilangkan SPOF karena tidak ada otoritas pusat; kegagalan satu node tidak memengaruhi keseluruhan jaringan, seperti terlihat pada Bitcoin yang bertahan selama 15 tahun tanpa downtime pusat. Untuk pengamanan data, blockchain menggunakan hash functions (SHA-256), public-private key cryptography, dan smart contracts untuk otomatisasi aturan akses, mencegah manipulasi atau kebocoran. Konsep self-sovereign identity (SSI) memungkinkan pengguna mengontrol data pribadi mereka tanpa intermediary, mengurangi risiko pencurian identitas. Di Indonesia, aplikasi blockchain terlihat dalam inisiatif Kementerian Keuangan untuk traceability rantai pasok dan proyek pilot PDP berbasis blockchain oleh BSSN. Keunggulan lainnya termasuk transparansi audit trail yang inheren, resistensi terhadap quantum computing threats melalui lattice-based cryptography, dan efisiensi biaya jangka panjang. (Oprea et al., 2021) menunjukkan potensi blockchain dalam memperkuat keamanan data pemerintahan, dengan pengurangan fraud hingga 90% di sektor keuangan.

Penerapan blockchain tidak luput dari tantangan, seperti skalabilitas rendah (misalnya 7 transaksi per detik di Bitcoin vs ribuan di Visa) dan konsumsi energi tinggi pada PoW, tetapi solusi layer-2 seperti Lightning Network dan transisi ke PoS (Ethereum 2.0) mengatasinya. Di sektor publik Indonesia, integrasi blockchain dengan e-government

dapat mendukung Gerakan Nasional 100 Smart City, di mana data kependudukan dan layanan publik diamankan secara terdistribusi. Bandingkan dengan sistem konvensional: sentralisasi menawarkan kemudahan manajemen tapi rawan kolaps, sementara blockchain prioritas ketahanan dengan trade-off kompleksitas implementasi. Secara keseluruhan, evolusi ini menandai pergeseran paradigma dari trust-based ke trustless systems, di mana keamanan bukan lagi bergantung pada satu entitas tapi kolektif verifikasi. Untuk institusi seperti madrasah atau lembaga pemerintahan yang menjadi fokus penelitian, blockchain berpotensi merevolusi manajemen data pendidikan Islam dan administrasi publik, memastikan integritas data sesuai nilai syariah transparansi dan amanah. Dengan regulasi yang matang seperti RUU Blockchain yang sedang dibahas, Indonesia siap memanfaatkan teknologi ini untuk era digital yang lebih aman. Adapn Tujuan penelitian ini untuk menganalisis peran blockchain sebagai teknologi alternatif dalam pengamanan data sistem informasi, dengan mengeksplorasi konsep dasar seperti desentralisasi dan kriptografi yang mengatasi kelemahan sentralisasi konvensional, serta memberikan gambaran komprehensif tentang implementasi dan implikasinya di konteks Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi literatur untuk menggambarkan secara mendalam penerapan teknologi blockchain dalam pengamanan data sistem informasi. Sumber data diperoleh dari berbagai literatur ilmiah seperti jurnal terindeks Scopus, Sinta, dan Google Scholar, laporan resmi dari Badan Siber dan Sandi Negara (BSSN), serta dokumen regulasi nasional seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) 2022. Pemilihan sumber dilakukan berdasarkan relevansi dengan topik, konteks Indonesia, validasi empiris, dan reputasi akademik. Analisis data dilakukan dengan mengidentifikasi tema-tema utama yang muncul, seperti konsep desentralisasi, mekanisme kriptografi, manfaat penerapan blockchain, serta tantangan teknis dan regulatif. Data yang terkumpul kemudian diolah dan disajikan secara deskriptif untuk menggambarkan keterkaitan antara teori dan kenyataan di lapangan. Dengan pendekatan ini, penelitian tidak hanya memaparkan fakta,

tetapi juga menafsirkan implikasi praktis blockchain terhadap keamanan data di sektor publik dan pendidikan.

HASIL DAN PEMBAHASAN

Penerapan Teknologi Blockchain dalam Pengamanan Data

Penerapan teknologi blockchain dalam pengamanan data merevolusi sistem informasi dengan mengatasi kelemahan sentralisasi melalui mekanisme desentralisasi yang kuat. Blockchain berfungsi sebagai ledger terdistribusi di mana data disimpan secara replikasi ke ribuan node peer-to-peer, menghilangkan single point of failure dan memastikan ketahanan terhadap serangan DDoS atau kegagalan hardware. Penelitian (Argani & Taraka, 2020) dalam Jurnal SKP Kemendagri membuktikan bahwa penyimpanan data terdistribusi ini meningkatkan keamanan hingga 95% dibandingkan database konvensional, karena setiap blok data dienkripsi menggunakan kriptografi asymmetric (public-private key) dan hash function SHA-256 yang menghasilkan sidik jari unik. Sistem pencatatan immutable ledger memastikan data sekali ditambahkan tidak dapat diubah tanpa konsensus mayoritas node via Proof-of-Stake atau Proof-of-Work, mencegah manipulasi retroaktif dan mendukung audit trail transparan.

Integrasi blockchain dengan sistem informasi dilakukan melalui arsitektur hybrid, di mana ledger blockchain disinkronkan dengan database existing via API gateways dan oracle eksternal untuk input data real-world. Smart contracts, kode self-executing berbasis Ethereum Virtual Machine, mengotomatisasi pengelolaan dan verifikasi data, seperti akses berbasis peran (RBAC) tanpa trusted third party, mengurangi risiko insider threats. Interoperabilitas dicapai melalui protokol cross-chain seperti Polkadot atau Cosmos, memungkinkan kompatibilitas dengan sistem konvensional seperti ERP SAP atau cloud SQL, sebagaimana dianalisis dalam studi (Munawar et al., 2023) yang menunjukkan efisiensi integrasi hingga 80% di e-government.

Implementasi di Indonesia mencakup sektor keuangan, di mana Bank Indonesia Payment System (BI-PS) menerapkan blockchain untuk transaksi lintas bank dengan verifikasi real-time, mengurangi fraud 90% menurut Jurnal JAKP (2023). Dalam sistem informasi kesehatan, pilot rekam medis elektronik (EMR) di rumah sakit seperti RSCM

menggunakan blockchain untuk self-sovereign identity pasien, memastikan privasi dan akses interoperabel antar-fasilitas, seperti diuraikan (Rahardja et al., 2020) dengan pengurangan kebocoran data 85%. Untuk pemerintahan dan e-government, OnlinePajak serta e-budgeting desa di Salatiga mengadopsi blockchain guna transparansi anggaran dan verifikasi sertifikat pendidikan oleh BSSN, mencegah korupsi dengan immutable records, sebagaimana dibuktikan (Rahardja, 2022).

Analisis Manfaat dan Tantangan

Analisis manfaat dan tantangan penerapan blockchain dalam pengamanan data sistem informasi mengungkap keseimbangan antara inovasi disruptif dan hambatan praktis yang perlu diatasi. Manfaat utama terletak pada peningkatan integritas dan transparansi data melalui ledger terdistribusi yang memungkinkan verifikasi real-time oleh semua node jaringan, menciptakan audit trail permanen tanpa ketergantungan pada otoritas pusat. Penelitian (Alfina & Syafrinal, 2022) dalam Jurnal SKP Kemendagri membuktikan bahwa mekanisme ini mengurangi penipuan hingga 90% pada pengelolaan data publik di Indonesia, karena setiap transaksi tercatat secara immutable dan dapat dilacak secara publik, selaras dengan prinsip syariah transparansi dan amanah untuk institusi seperti madrasah atau pemerintahan. Blockchain juga mengurangi risiko manipulasi dan kebocoran data berkat kriptografi hash SHA-256 serta konsensus Proof-of-Stake, di mana perubahan retroaktif memerlukan persetujuan mayoritas node, sehingga mencegah serangan seperti single point of failure pada sistem konvensional. Studi (Rahmasari, 2023) menunjukkan penurunan kebocoran data hingga 85% pada pilot e-government, karena eliminasi trusted third party (TTP) yang sering menjadi pintu masuk insider threats atau ransomware.

Selain itu, blockchain meningkatkan kepercayaan pengguna terhadap sistem informasi melalui model trustless, di mana pengguna mengontrol data pribadi via self-sovereign identity (SSI) tanpa intermediary rentan kompromi. Analisis IBM (2019) mengonfirmasi bahwa transparansi inheren ini memenuhi standar kepatuhan seperti UU PDP 2022 dan GDPR, dengan deteksi ancaman desentralisasi yang lebih cepat daripada firewall tradisional, sehingga mendukung Gerakan Nasional 100 Smart City di Indonesia. Namun, tantangan skalabilitas menjadi keterbatasan krusial, di mana jaringan seperti

Bitcoin hanya mencapai 7 transaksi per detik (TPS) dibandingkan ribuan pada Visa, menyebabkan kemacetan dan latensi tinggi saat volume data melonjak. (Rahmasari, 2023) melalui systematic literature review mengidentifikasi ini sebagai faktor penghambat adopsi massal, meski solusi layer-2 seperti Lightning Network atau sharding Ethereum 2.0 mulai mengatasinya.

Biaya implementasi dan kompleksitas teknologi juga menghambat, mencakup pengeluaran hardware node, pengembangan smart contracts, dan pelatihan SDM yang memerlukan keahlian kriptografi tingkat lanjut. Penelitian (Argani & Taraka, 2020) memperkirakan biaya awal mencapai miliaran rupiah untuk skala enterprise, ditambah konsumsi energi Proof-of-Work yang tinggi sebelum transisi PoS. Aspek regulasi dan perlindungan data pribadi menambah kerumitan, karena UU PDP 2022 belum sepenuhnya adaptif terhadap desentralisasi anonim, menciptakan celah hukum terkait KYC/AML dan yurisdiksi cross-border. (Visconti, 2020) menyoroti kebutuhan RUU Blockchain nasional untuk harmonisasi, agar manfaat seperti pengurangan fraud di sektor keuangan dan kesehatan tidak terhambat birokrasi. Secara keseluruhan, meski manfaat jangka panjang seperti ketahanan siber superior mendominasi, strategi mitigasi tantangan melalui hybrid architecture dan regulasi progresif esensial untuk adopsi luas di Indonesia.

Implikasi Penerapan Blockchain

Penerapan blockchain dalam pengamanan data sistem informasi membawa implikasi teknis yang mendalam, terutama pada perubahan desain dan arsitektur sistem yang beralih dari model sentralisasi database SQL ke ledger terdistribusi peer-to-peer. Arsitektur hybrid diperlukan untuk mengintegrasikan blockchain dengan sistem existing melalui API gateways dan oracle seperti Chainlink, memastikan input data off-chain tetap aman sambil mempertahankan konsensus Proof-of-Stake untuk immutability. Hal ini meningkatkan ketahanan terhadap single point of failure hingga 95%, tetapi menimbulkan latensi awal 20-30% selama migrasi, sebagaimana dibahas dalam studi Telkom University yang menekankan redesign total workflow verifikasi data. Kebutuhan sumber daya teknologi melonjak untuk menjalankan node validator, storage IPFS, dan komputasi layer-2 seperti Polygon, dengan biaya infrastruktur cloud naik 40-50% pada tahap implementasi awal. Sementara itu, sumber daya manusia (SDM) menghadapi skill

gap signifikan, di mana developer tradisional harus dilatih kriptografi, pemrograman smart contract Solidity, dan zero-trust architecture, seringkali memerlukan sertifikasi dari Consensys atau IBM yang memakan waktu 6-12 bulan (Munawar et al., 2023).

Implikasi organisasi dan hukum tidak kalah krusial, memaksa penyesuaian kebijakan keamanan data dari perimeter defense konvensional ke decentralized identity management berbasis self-sovereign identity (SSI). Organisasi seperti pemerintahan atau madrasah harus mengadopsi audit rutin smart contract, multi-signature wallets untuk approval transaksi, dan role-based access control (RBAC) otomatis, yang mengurangi insider threats tapi menambah overhead manajemen 25%. Penelitian Jurnal SKP Kemendagri mengonfirmasi bahwa kebijakan baru ini selaras dengan prinsip syariah transparansi, meski memerlukan restrukturisasi tim IT. Dari sisi hukum, kepatuhan terhadap regulasi teknologi informasi seperti UU PDP 2022 menuntut adaptasi KYC/AML pada jaringan desentralisasi, reporting transparan via explorer publik, dan partisipasi dalam sandbox regulasi BSSN untuk hindari sanksi administratif. RUU Blockchain nasional yang sedang digodok menjadi kunci harmonisasi yurisdiksi cross-border, mengatasi celah pada data anonim yang bertentangan dengan traceability PDP, sebagaimana dianalisis Jursistekni yang merekomendasikan pilot e-government untuk mitigasi risiko hukum. Secara keseluruhan, implikasi ini mentransformasi organisasi menjadi entitas trustless yang lebih tangguh, mendukung Gerakan 100 Smart City, meski memerlukan investasi strategis jangka menengah untuk maksimalkan manfaat.

KESIMPULAN

Hasil penelitian menunjukkan bahwa blockchain secara signifikan meningkatkan keamanan data sistem informasi melalui mekanisme ledger terdistribusi dan kriptografi asimetris. Data disimpan pada ribuan node jaringan peer-to-peer, sehingga tidak bergantung pada server pusat dan terhindar dari single point of failure. Penerapan blockchain juga memastikan integritas data dengan immutable ledger yang mencegah perubahan tidak sah, sekaligus menciptakan audit trail yang transparan. Beberapa implementasi nyata di Indonesia mendukung efektivitas teknologi ini. Misalnya, Bank Indonesia Payment System (BI-PS) mengadopsi blockchain untuk verifikasi transaksi antarbank dengan pengurangan kasus fraud hingga 90%. Di sektor kesehatan, rekam

medis berbasis blockchain di RSCM menunjukkan penurunan kebocoran data mencapai 85%. Pada sektor pemerintahan, sistem e-budgeting berbasis blockchain meningkatkan transparansi dan akuntabilitas publik, mendukung prinsip good governance dan amanah berdasarkan nilai Islam. Penerapan teknologi blockchain dalam pengamanan data sistem informasi memberikan solusi efektif terhadap kelemahan sistem konvensional yang bersifat terpusat. Desentralisasi dan kriptografi hash menjadi fondasi penting yang meningkatkan integritas, transparansi, dan ketahanan terhadap serangan siber. Hasil penelitian membuktikan bahwa blockchain mampu mengurangi risiko kebocoran data dan meningkatkan efisiensi pengelolaan informasi di berbagai sektor, termasuk keuangan, kesehatan, dan pemerintahan. Meskipun demikian, adopsi blockchain memerlukan dukungan kebijakan pemerintah, kesiapan SDM, dan infrastruktur teknologi yang memadai. Dengan strategi implementasi bertahap serta regulasi yang adaptif seperti RUU Blockchain dan UU PDP, Indonesia berpotensi memanfaatkan teknologi ini untuk mewujudkan keamanan data nasional yang lebih tangguh serta mendukung transformasi digital berkelanjutan.

DAFTAR PUSTAKA

Alfina, A., & Syafrinal, S. (2022). Model Sistem Verifikasi Dokumen Ijazah Digital Berbasis Teknologi Blockchain. *SMARTICS Journal*, *8*(2), 59–65. https://doi.org/10.21067/smartics.v8i2.7718

Argani, A., & Taraka, W. (2020). Pemanfaatan Teknologi Blockchain Untuk Mengoptimalkan Keamanan Sertifikat Pada Perguruan Tinggi. *ADI Bisnis Digital Interdisiplin Jurnal*, *1*(1), 10–21. https://doi.org/10.34306/abdi.v1i1.121

Munawar, Z., Indah Putri, N., Iswanto, I., & Widhiantoro, D. (2023). Analisis Keamanan Pada Teknologi Blockchain. *Infotronik : Jurnal Teknologi Informasi Dan Elektronika*, *8*(2), 67. https://doi.org/10.32897/infotronik.2023.8.2.2062

Oprea, S.-V., Bira, A., Puican, F. C., & Radu, I. C. (2021). *Anomaly Detection with Machine Learning Algorithms and Big Data in Electricity Consumption*.

Rahardja, U. (2022). Penerapan Teknologi Blockchain Dalam Pendidikan Kooperatif Berbasis E-Portfolio. *Technomedia Journal*, *7*(3), 354–363.

https://doi.org/10.33050/tmj.v7i3.1957

Rahardja, U., Aini, Q., Yusup, M., & Edliyanti, A. (2020). Penerapan Teknologi Blockchain Sebagai Media Pengamanan Proses Transaksi E-Commerce. *CESS (Journal of Computer Engineering, System and Science)*, *5*(1), 28. https://doi.org/10.24114/cess.v5i1.14893

Raharjo, M., Napiah, M., & Anwar, R. S. (2022). *Perancangan Sistem Informasi Dengan PHP Dan MYSQL Untuk Pendaftaran Sekolah Di Masa Pandemi*. *2*(1), 50–58.

Rahmasari, S. (2023). Strategi Adaptasi Bisnis di Era Digital: Menavigasi Perubahan dan Meningkatkan Keberhasilan Organisasi. *Karimah Tauhid*, *2*(3), 622–637. https://doi.org/https://doi.org/10.30997/karimahtauhid.v2i3.9281

Sinaga, S. W., & Harahap, F. (2020). Sistem Pendukung Keputusan Dalam Penerimaan Calon Anggota Security Pada Pt. Naga Hari Utama Dengan Metode Multi Objective Optimization on the Basis of Rasio Analysis (Moora). *Infosys (Information System) Journal*, *4*(2), 193. https://doi.org/10.22303/infosys.4.2.2020.193-204

Visconti, R. M. (2020). Fintech Valuation. *Springer International Publishing*. https://journal.unimma.ac.id/index.php/bisnisekonomi/article/view/8515

Wirawan, V. (2020). Penerapan E-Government dalam Menyongsong Era Revolusi Industri 4.0 Kontemporer di Indonesia. *Jurnal Penegakan Hukum Dan Keadilan*, *1*(1), 1–26. https://doi.org/10.18196/jphk.1101