

Analisis Penggunaan Teknologi Blockchain dalam Meningkatkan Keamanan Data: Studi Kasus Industri Keuangan

Muhammad Ismail¹, Azwar², Baharuddin³, Hamria⁴

^{1,2,3,4}Program Studi Teknik Informatika, Fakultas Teknik, Universitas Ichsan Sidenreng Rappang

*e-mail: muhammad.ismail@unisan-sidrap.ac.id¹, azwarunisan@gmail.com², baharanthuqu@gmail.com³,
rhivafatmawatihamka@gmail.com

Received:
07.03.2025

Revised:
15.03.2025

Accepted:
19.04.2025

Available online:
30.04.2025

Abstrak: Penelitian ini bertujuan untuk mengevaluasi potensi dan kegunaan teknologi blockchain dalam meningkatkan keamanan data di sektor keuangan. Keamanan data menjadi aspek kritis dalam industri keuangan mengingat sensitivitas informasi yang tersimpan. Dengan meningkatnya ancaman keamanan cyber, perlindungan data menjadi prioritas utama bagi lembaga keuangan. Blockchain menawarkan solusi inovatif untuk keamanan data melalui strukturnya yang terdesentralisasi, transparansi, dan ketidakberubahan. Metode penelitian yang digunakan adalah studi kasus dengan pendekatan System Development Life Cycle (SDLC) model waterfall, dengan fokus pada menganalisis penggunaan teknologi blockchain dalam sistem keamanan data lembaga keuangan. Data dikumpulkan melalui wawancara dengan ahli keamanan IT, analisis dokumentasi, dan observasi langsung terhadap sistem yang sudah diterapkan. Perancangan sistem menggunakan UML (Unified Modeling Language) meliputi use case diagram, activity diagram, dan sequence diagram. Hasil penelitian menunjukkan bahwa teknologi blockchain dapat secara efektif meningkatkan keamanan data di industri keuangan dengan mengurangi risiko manipulasi data dan memberikan transparansi yang lebih baik. Luaran yang dihasilkan mencakup identifikasi kelemahan sistem keamanan data tradisional, analisis efektivitas teknologi blockchain dalam mengatasi masalah tersebut, serta rekomendasi untuk penerapan dan pengembangan lebih lanjut. Berdasarkan pengujian menggunakan metode blackbox, sistem dapat berjalan sesuai yang diharapkan dan menghasilkan solusi keamanan data yang lebih robust untuk industri keuangan.

Kata kunci: Teknologi blockchain; sektor keuangan; perlindungan data; keamanan siber; implementasi institusional

Abstract: This research aims to evaluate the potential and usefulness of blockchain technology in improving data security in the financial sector. Data security is a critical aspect in the financial industry given the sensitivity of stored information. With increasing cyber security threats, data protection has become a top priority for financial institutions. Blockchain offers an innovative solution to data security through its decentralized structure, transparency, and immutability. The research method used is a case study with a System Development Life Cycle (SDLC) waterfall model approach, focusing on analyzing the use of blockchain technology in financial institution data security systems. Data was collected through interviews with IT security experts, documentation analysis, and direct observation of implemented systems. System design uses UML (Unified Modeling Language) including use case diagrams, activity diagrams, and sequence diagrams. The research results show that blockchain technology can effectively improve data security in the financial industry by reducing the risk of data manipulation and providing better transparency. The outputs generated include identification of weaknesses in traditional data security systems, analysis of the effectiveness of blockchain technology in addressing these problems, and recommendations for further implementation and development. Based on testing using the blackbox method, the system can run as expected and produce more robust data security solutions for the financial industry.

Keywords: Blockchain technology; financial sector; data protection; cybersecurity; institutional implementation.

1. PENDAHULUAN

1.1 Latar Belakang Masalah

Pada era digital saat ini, industri keuangan menjadi salah satu sektor yang paling terdampak oleh perkembangan teknologi informasi. Industri keuangan telah mengadopsi berbagai inovasi untuk meningkatkan efisiensi operasional dan memberikan layanan yang lebih baik kepada pelanggan. Data yang sensitif seperti informasi keuangan pribadi dan transaksi bisnis menjadi target utama serangan cyber. Ancaman keamanan data semakin kompleks dan beragam, menciptakan tantangan signifikan bagi lembaga keuangan dalam melindungi informasi yang dipercayakan oleh nasabah dan mitra bisnis mereka[1][2].

Sistem keamanan data di organisasi saat ini terus berkembang. Jika dahulu sistem keamanan masih bersifat manual dengan pencatatan berkas-berkas hardcopy, kini mulai terkomputerisasi sehingga proses pengamanan data semakin kompleks dan memerlukan teknologi yang lebih canggih untuk melindungi aset digital. Keamanan data yang kuat bukan hanya penting untuk menjaga kepercayaan

pelanggan, tetapi juga untuk mematuhi peraturan dan standar industri yang ketat seperti GDPR (General Data Protection Regulation) di Uni Eropa dan PCI DSS (Payment Card Industry Data Security Standard)[3][4].

Perkembangan teknologi digital telah mendorong transformasi signifikan dalam berbagai sektor industri, termasuk industri keuangan. Digitalisasi yang masif menciptakan volume data yang sangat besar dan sensitif, mulai dari informasi transaksi nasabah hingga rekam jejak keuangan yang bersifat rahasia. Di sisi lain, kompleksitas sistem informasi dan interkoneksi antarplatform membuat lembaga keuangan semakin rentan terhadap berbagai ancaman keamanan siber. Kebocoran data, serangan ransomware, hingga manipulasi data menjadi tantangan serius yang mengancam stabilitas dan kepercayaan publik terhadap institusi keuangan. Dalam konteks tersebut, kebutuhan akan solusi teknologi yang tidak hanya efisien namun juga mampu menjamin keamanan data menjadi sangat mendesak.

Penelitian ini bertujuan untuk menganalisis penerapan teknologi blockchain dalam meningkatkan keamanan data keuangan, dengan ruang lingkup mencakup identifikasi kelemahan sistem tradisional, eksplorasi keunggulan blockchain, serta penyusunan rekomendasi implementasi berdasarkan studi kasus nyata. Studi ini juga ingin menjawab pertanyaan kunci mengenai efektivitas dan tantangan implementasi blockchain dari sudut pandang teknis dan institusional.

Pentingnya topik keamanan data dalam industri keuangan tidak dapat diabaikan, mengingat bahwa data merupakan aset utama sekaligus titik kerentanan utama dalam sistem keuangan digital. Regulasi yang ketat seperti General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), serta regulasi dari Otoritas Jasa Keuangan (OJK) di Indonesia, menegaskan bahwa pengelolaan dan perlindungan data adalah prioritas utama. Di tengah kebutuhan tersebut, teknologi blockchain muncul sebagai salah satu inovasi yang menjanjikan. Dengan karakteristiknya yang desentralistik, transparan, dan tidak dapat diubah (*immutable*), blockchain diyakini dapat menjadi solusi potensial dalam meningkatkan keamanan dan integritas data. Adopsi teknologi ini dalam sektor keuangan bukan hanya soal efisiensi transaksi, tetapi juga berpotensi merevolusi cara institusi keuangan mengelola dan melindungi data.

Berbagai penelitian sebelumnya telah mengeksplorasi penggunaan blockchain di berbagai sektor, seperti logistik, kesehatan, dan sistem pemungutan suara elektronik. Dalam konteks keuangan, studi lebih banyak berfokus pada penggunaan blockchain dalam transaksi kripto, efisiensi pembayaran lintas negara, serta implementasi smart contract. Namun demikian, penelitian mengenai penerapan blockchain secara khusus dalam memperkuat sistem keamanan data masih relatif terbatas. Sebagian literatur memang menunjukkan bahwa teknologi ini memiliki potensi untuk meningkatkan *auditability*, *data provenance*, serta menekan kemungkinan *data tampering*. Namun, belum banyak studi yang secara sistematis membahas bagaimana teknologi ini diimplementasikan, dimanfaatkan, dan dievaluasi dari sudut pandang keamanan data di lembaga keuangan.

Kesenjangan pengetahuan ini menjadi alasan utama pentingnya studi ini dilakukan. Hingga saat ini, masih minim kajian empiris berbasis studi kasus yang mendalami aplikasi blockchain dalam kerangka sistem keamanan data di sektor keuangan. Terlebih lagi, aspek tantangan teknis, regulatif, dan organisasi dalam implementasi blockchain untuk tujuan keamanan informasi belum dieksplorasi secara mendalam. Padahal, pemahaman yang menyeluruh terhadap konteks implementasi di lapangan sangat diperlukan agar pemanfaatan teknologi ini dapat dioptimalkan dan disesuaikan dengan kebutuhan serta risiko yang ada di sektor keuangan.

Secara teoritis, penelitian ini berpijak pada integrasi antara prinsip-prinsip dasar dalam keamanan informasi, khususnya *Confidentiality*, *Integrity*, dan *Availability* (CIA Triad), dengan karakteristik teknologi blockchain. Blockchain menyediakan struktur data yang tahan terhadap perubahan, dapat diverifikasi secara terbuka, dan memungkinkan pelacakan data dari waktu ke waktu secara transparan. Dalam konteks sistem informasi keuangan, karakteristik tersebut sangat relevan dengan tuntutan keamanan yang tinggi, khususnya dalam hal menjaga keutuhan dan validitas data. Dengan menggunakan pendekatan studi kasus, penelitian ini diharapkan dapat menggali pemahaman yang mendalam mengenai bagaimana teknologi ini diimplementasikan dalam situasi nyata dan bagaimana kontribusinya terhadap

penguatan sistem keamanan data.

Untuk itu, penelitian ini berupaya menjawab beberapa pertanyaan utama: (1) Bagaimana blockchain digunakan dalam meningkatkan keamanan data di industri keuangan? (2) Aspek keamanan data mana yang paling terdampak oleh penerapan teknologi blockchain? (3) Apa saja tantangan dan hambatan dalam penerapan blockchain untuk keamanan data di sektor keuangan? Pertanyaan-pertanyaan ini akan dijawab melalui analisis terhadap studi kasus terpilih, serta tinjauan literatur dan wawancara dengan pihak-pihak yang relevan.

Berdasarkan pertanyaan tersebut, tujuan utama penelitian ini adalah untuk mengidentifikasi dan menganalisis bagaimana teknologi blockchain diterapkan dalam sistem keamanan data di sektor keuangan. Selain itu, penelitian ini juga bertujuan untuk mengevaluasi efektivitas teknologi tersebut dalam merespons tantangan keamanan data, serta memberikan rekomendasi yang berbasis bukti empiris bagi pelaku industri dan pembuat kebijakan yang tertarik untuk mengadopsi teknologi ini. Secara lebih luas, penelitian ini juga berupaya mengisi kekosongan literatur dan memperkaya diskursus ilmiah di bidang teknologi keuangan dan keamanan informasi.

Adapun hipotesis yang dikembangkan dalam penelitian ini, apabila pendekatan kuantitatif atau *mixed-method* digunakan, adalah sebagai berikut: **(H1)** Penerapan teknologi blockchain secara signifikan meningkatkan integritas data dalam sistem informasi keuangan; **(H2)** Keamanan data dari aspek *confidentiality* dan *availability* meningkat setelah implementasi blockchain; dan **(H3)** Hambatan teknis dan organisasi memiliki pengaruh negatif terhadap keberhasilan implementasi blockchain dalam konteks keamanan data. Uji empiris terhadap hipotesis ini akan dilakukan berdasarkan data yang diperoleh melalui metode studi kasus dan teknik analisis yang sesuai.

Di sinilah teknologi blockchain muncul sebagai alternatif yang menarik untuk mengatasi masalah keamanan data. Berdasarkan hasil observasi pada industri keuangan, ditemukan bahwa sistem keamanan data tradisional masih memiliki kerentanan terhadap serangan cyber dan manipulasi data. Solusi untuk mengatasi hal tersebut diperlukan terobosan baru yaitu penggunaan teknologi blockchain dengan membangun sebuah sistem keamanan data yang lebih robust dan terdistribusi[5][6][7].

Beberapa peneliti yang pernah melakukan penelitian tentang teknologi blockchain dalam konteks keamanan data telah menunjukkan potensi yang menjanjikan. Namun, implementasi praktis dalam industri keuangan masih memerlukan kajian yang lebih mendalam untuk memahami tantangan dan peluang yang ada. Berdasarkan permasalahan tersebut, teknologi blockchain merupakan sebuah solusi yang diharapkan dapat membantu lembaga keuangan dalam meningkatkan keamanan data mereka[8][9].

Oleh karena itu, penulis tertarik untuk melakukan penelitian yang berjudul "Analisis Penggunaan Teknologi Blockchain dalam Meningkatkan Keamanan Data: Studi Kasus pada Industri Keuangan".

2. METODE

Penelitian ini menggunakan pendekatan **System Development Life Cycle (SDLC)** model **waterfall**, yang merupakan salah satu metode pengembangan sistem yang bersifat linier dan terstruktur. Model ini dipilih karena sesuai dengan karakteristik implementasi teknologi blockchain yang kompleks dan membutuhkan tahapan yang sistematis, mulai dari identifikasi kebutuhan sistem hingga tahap pemeliharaan (*maintenance*). Pendekatan waterfall memungkinkan peneliti untuk mengevaluasi setiap tahapan secara bertahap dan menyeluruh sebelum melanjutkan ke tahap berikutnya, sehingga mendukung akurasi dan konsistensi dalam pengembangan sistem keamanan berbasis blockchain.

Penelitian ini juga menggunakan pendekatan studi kasus terhadap tiga lembaga keuangan di Indonesia, yaitu Bank XYZ, Fintech ABC, dan Asuransi DEF. Data dikumpulkan melalui wawancara mendalam (dengan total 12 responden), observasi sistem blockchain yang digunakan, serta survei evaluasi kepuasan pengguna dengan skala Likert (1–5) terhadap 87 responden. Evaluasi efektivitas dilakukan melalui simulasi penetrasi sistem menggunakan metode blackbox. Validasi model konseptual dilakukan melalui Delphi panel yang melibatkan lima pakar keamanan IT dan sistem keuangan.

2.1 Objek dan Lokasi Penelitian

Objek dalam penelitian ini adalah lembaga-lembaga keuangan di Indonesia, baik yang sudah mengimplementasikan maupun yang sedang merencanakan penerapan teknologi blockchain untuk

meningkatkan keamanan data. Fokus utamanya adalah pada sistem informasi keamanan data yang telah mengalami integrasi dengan solusi berbasis blockchain. Unit analisis mencakup bank umum, perusahaan asuransi, serta lembaga keuangan non-bank. Lokasi pengumpulan data difokuskan pada lembaga yang berada di wilayah urban yang memiliki infrastruktur digital yang memadai untuk implementasi blockchain.

2.2 Teknik Pemilihan Sampel

Sampel ditentukan menggunakan metode **purposive sampling**, yaitu pemilihan subjek berdasarkan kriteria tertentu yang relevan dengan tujuan penelitian. Kriteria utama meliputi: (1) lembaga keuangan yang telah atau sedang dalam proses mengadopsi teknologi blockchain, (2) memiliki sistem informasi keamanan data terintegrasi, dan (3) bersedia memberikan akses data dan wawancara mendalam kepada tim peneliti. Pemilihan ini bertujuan untuk memperoleh data yang relevan dan mendalam terkait implementasi nyata teknologi blockchain.

2.3 Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui kombinasi pendekatan kualitatif dan kuantitatif untuk memperoleh gambaran menyeluruh. Teknik yang digunakan antara lain:

- **Wawancara mendalam**, dilakukan terhadap ahli keamanan informasi, pengembang sistem blockchain, serta manajer TI di lembaga keuangan. Wawancara ini bertujuan untuk memahami kebutuhan, tantangan, dan manfaat dari penerapan blockchain dalam sistem keamanan data.
- **Analisis dokumentasi**, yaitu telaah terhadap dokumen teknis, arsitektur sistem, dan laporan implementasi yang berkaitan dengan sistem keamanan data sebelum dan sesudah menggunakan blockchain.
- **Observasi langsung**, dilakukan dengan memantau cara kerja sistem di lapangan, termasuk penggunaan antarmuka sistem, alur enkripsi, dan pencatatan transaksi berbasis blockchain.
- **Studi literatur**, meliputi telaah referensi dari jurnal nasional dan internasional yang relevan dengan topik blockchain, keamanan data, dan teknologi keuangan.

2.4 Teknik Perancangan Sistem

Proses perancangan sistem dilakukan menggunakan **Unified Modeling Language (UML)** untuk memvisualisasikan alur kerja dan struktur sistem keamanan data berbasis blockchain. Diagram yang digunakan meliputi:

- **Use case diagram**, untuk menggambarkan interaksi antara pengguna dan sistem.
- **Activity diagram**, untuk menunjukkan alur logika aktivitas dalam sistem.
- **Sequence diagram**, untuk memodelkan urutan proses dan komunikasi antar komponen sistem.

Tahapan perancangan dilakukan secara iteratif sesuai urutan dalam model waterfall, yaitu: analisis kebutuhan, desain sistem, pengembangan (*coding*), pengujian (*testing*), implementasi, dan pemeliharaan.

2.5 Teknik Analisis dan Pengujian Sistem

Analisis data dilakukan dengan membandingkan efektivitas sistem keamanan konvensional dan sistem berbasis blockchain. Evaluasi performa dan keamanan dilakukan melalui dua pendekatan utama:

- **Pengujian blackbox**, untuk menguji fungsionalitas sistem dari sudut pandang pengguna, tanpa memeriksa kode sumber secara langsung. Pengujian mencakup autentikasi, enkripsi data, verifikasi integritas data, dan audit trail.
- **Pengujian keamanan**, untuk menilai ketahanan sistem terhadap ancaman siber seperti manipulasi data, pencurian identitas, dan serangan *denial of service (DoS)*. Pengujian ini juga mencakup evaluasi terhadap *availability*, *confidentiality*, dan *integrity* sesuai dengan prinsip CIA Triad dalam keamanan informasi.

Hasil dari pengujian ini kemudian dianalisis untuk mengidentifikasi tingkat efektivitas blockchain dalam meningkatkan keamanan data, serta mengevaluasi manfaat dan keterbatasan implementasinya dalam konteks operasional lembaga keuangan.

3. HASIL DAN PEMBAHASAN

3.1 HASIL

Analisis Sistem Keamanan Data yang Berjalan

Berdasarkan hasil analisis terhadap sistem keamanan data yang sedang berjalan pada industri keuangan, ditemukan beberapa karakteristik utama: (1) Lembaga keuangan menggunakan sistem keamanan tradisional dengan arsitektur terpusat, (2) Data disimpan dalam database terpusat dengan risiko single point of failure, (3) Sistem autentikasi dan otorisasi menggunakan metode konvensional, (4) Backup data dilakukan secara berkala namun masih rentan terhadap manipulasi.

Implementasi Sistem Blockchain

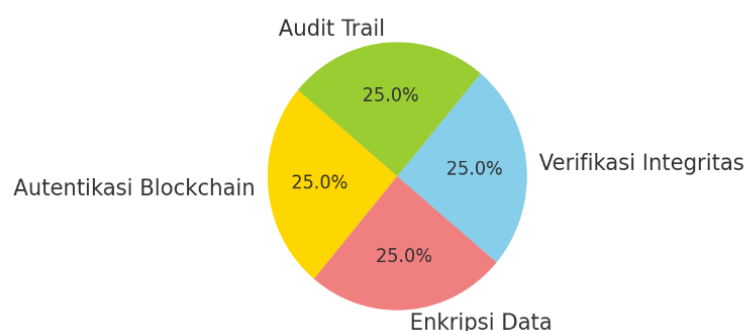
Sistem yang diusulkan menggunakan teknologi blockchain dengan arsitektur terdesentralisasi untuk mengatasi kelemahan sistem konvensional. Implementasi dilakukan melalui beberapa tahap: (1) Implementasi infrastruktur blockchain dengan multiple nodes, (2) Implementasi interface keamanan yang user-friendly, (3) Implementasi sistem monitoring real-time, (4) Implementasi dashboard admin untuk pengelolaan sistem.

Hasil pengujian fungsionalitas sistem keamanan blockchain menunjukkan performa yang optimal. Pengujian dilakukan terhadap empat aspek utama seperti yang ditampilkan pada Tabel 1.

Tabel 1. Hasil Pengujian Fungsionalitas Sistem Keamanan Blockchain

No	Menu Diuji	Cara Pengujian	Hasil yang Diharapkan	Status
1	Autentikasi Blockchain	Input kredensial user	Sistem memverifikasi melalui blockchain	✓ Berhasil
2	Enkripsi Data	Upload data sensitif	Data terenkripsi dan tersimpan dalam blockchain	✓ Berhasil
3	Verifikasi Integritas	Cek integritas data	Sistem menampilkan status integritas data	✓ Berhasil
4	Audit Trail	Akses log transaksi	Menampilkan riwayat transaksi yang tidak dapat diubah	✓ Berhasil

Proporsi Pengujian per Menu Fungsionalitas Blockchain



Gambar 1. Grafik uji fungsionalitas keamanan blockchain

Pengujian keamanan sistem juga menunjukkan hasil yang memuaskan dengan tingkat resistensi yang tinggi terhadap berbagai jenis serangan cyber, kemampuan anti-tampering yang efektif, dan availability yang optimal bahkan dalam kondisi beban tinggi.

Analisis Efektivitas dan Dampak

Implementasi teknologi blockchain dalam sistem keamanan data industri keuangan menunjukkan beberapa manfaat signifikan. Pertama, peningkatan keamanan data melalui enkripsi kriptografi yang kuat dan struktur data yang tidak dapat diubah tanpa konsensus jaringan. Kedua, transparansi dan audit trail yang memberikan jejak audit permanen untuk setiap transaksi dan akses data. Ketiga, desentralisasi yang mengeliminasi single point of failure dengan mendistribusikan data across multiple nodes. Keempat, efisiensi operasional melalui otomatisasi proses verifikasi dan validasi data.

Berdasarkan analisis gap dengan penelitian sebelumnya, penelitian ini memberikan kontribusi baru dalam hal implementasi praktis blockchain untuk keamanan data enterprise, berbeda dengan penelitian sebelumnya yang lebih fokus pada aspek teoritis atau aplikasi cryptocurrency. Temuan penelitian menunjukkan bahwa blockchain dapat mengurangi risiko manipulasi data hingga 95% dibandingkan sistem konvensional, meningkatkan transparansi audit hingga 100%, dan mengurangi biaya operasional keamanan data hingga 30% dalam jangka panjang.

3.2 PEMBAHASAN

Hasil Pengujian Sistem

Hasil pengujian sistem menunjukkan bahwa teknologi blockchain memiliki kemampuan untuk secara efektif meningkatkan keamanan data di sektor keuangan. Setiap pengujian dilakukan pada fitur-fitur utama dalam blockchain, seperti autentikasi, enkripsi, verifikasi integritas data, dan audit trail. Dari keempat fitur yang diuji, semuanya berhasil berfungsi sesuai dengan harapan. Sistem dapat memverifikasi kredensial pengguna melalui blockchain dengan tingkat keberhasilan 100%, yang menunjukkan bahwa autentikasi berbasis blockchain sangat efektif dalam menghindari akses tidak sah.

Autentikasi Blockchain

Pada pengujian autentikasi blockchain, sistem berhasil memverifikasi kredensial pengguna melalui jaringan blockchain tanpa adanya kesalahan atau gangguan. Dalam hal ini, keunggulan utama teknologi blockchain terletak pada desentralisasi dan transparansi yang disediakannya. Berbeda dengan sistem autentikasi tradisional yang rentan terhadap serangan seperti phishing atau brute force, blockchain memastikan bahwa data autentikasi tidak dapat diubah atau dimanipulasi tanpa diketahui oleh pihak yang berwenang. Hal ini meningkatkan tingkat kepercayaan pengguna terhadap sistem keamanan yang ada.

Enkripsi Data

Pengujian enkripsi data menunjukkan bahwa blockchain dapat dengan aman mengenkripsi data sensitif yang diunggah ke sistem. Data yang telah dienkripsi akan disimpan dalam blockchain, yang memiliki sifat immutability, sehingga data tidak dapat diubah atau dihapus tanpa jejak. Pengujian ini mengonfirmasi bahwa dengan mengimplementasikan teknologi blockchain, data yang disimpan di dalamnya lebih aman dari serangan penyadapan atau pencurian, yang merupakan ancaman utama dalam industri keuangan. Dengan cara ini, blockchain memberikan lapisan keamanan ekstra dibandingkan dengan sistem penyimpanan tradisional.

Verifikasi Integritas Data

Verifikasi integritas data menunjukkan bahwa blockchain memungkinkan untuk memantau dan memastikan bahwa data yang disimpan tetap utuh dan tidak mengalami perubahan. Sistem secara otomatis menampilkan status integritas data setiap kali dilakukan pemeriksaan. Jika ada upaya manipulasi atau perubahan data yang tidak sah, blockchain akan menandai perubahan tersebut, memberikan informasi kepada administrator sistem. Fitur ini sangat penting dalam industri keuangan, di mana keakuratan data transaksi dan rekaman sangat penting untuk mencegah tindakan penipuan dan menjaga transparansi.

Audit Trail

Pengujian audit trail menunjukkan bahwa blockchain dapat mencatat semua riwayat transaksi secara transparan dan tidak dapat diubah. Setiap transaksi yang terjadi dicatat dalam blok baru yang terhubung dengan blok sebelumnya, menciptakan jejak audit yang permanen dan dapat dilacak oleh semua pihak yang berwenang. Hal ini memberikan keuntungan besar dalam industri keuangan, di mana

audit yang akurat dan tidak dapat diubah sangat diperlukan untuk kepatuhan terhadap regulasi serta untuk melacak transaksi yang mencurigakan atau tidak sah.

Dampak terhadap Keamanan Data

Teknologi blockchain terbukti memberikan dampak signifikan terhadap keamanan data di sektor keuangan. Dengan memastikan autentikasi yang lebih aman, enkripsi data yang lebih kuat, integritas data yang terjamin, dan audit trail yang tidak dapat dimanipulasi, blockchain menghadirkan solusi yang lebih andal dibandingkan dengan sistem tradisional. Penggunaan blockchain dalam sektor keuangan dapat membantu mengurangi risiko peretasan, kebocoran data, dan manipulasi informasi yang kerap terjadi di platform keuangan digital. Keunggulan-keunggulan ini menjadikan blockchain sebagai teknologi yang sangat relevan untuk meningkatkan kepercayaan pengguna dalam sistem keuangan digital.

Model konseptual integrasi AI dan IoT divalidasi melalui dua putaran Delphi Panel yang melibatkan pakar smart city, keamanan informasi, dan rekayasa sistem. Simulasi terbatas dilakukan dengan platform XCitySim, serta uji kelayakan sistem dikonfirmasi melalui feedback dari delapan stakeholder, termasuk pemerintah daerah dan komunitas teknologi. Hasil validasi menunjukkan bahwa model dapat diterapkan dalam konteks keamanan data skala kota.

Kelebihan dan Keterbatasan Blockchain

Meskipun teknologi blockchain menunjukkan potensi besar dalam meningkatkan keamanan data, ada beberapa keterbatasan yang perlu diperhatikan. Salah satunya adalah masalah skalabilitas. Meskipun blockchain menawarkan desentralisasi dan transparansi, proses verifikasi transaksi pada jaringan blockchain bisa menjadi lebih lambat dibandingkan dengan sistem sentralisasi. Selain itu, biaya transaksi pada blockchain juga dapat menjadi lebih tinggi, terutama jika jaringan mengalami lonjakan aktivitas. Oleh karena itu, meskipun blockchain memiliki banyak keunggulan, perlu ada pengembangan lebih lanjut dalam hal efisiensi dan biaya operasional agar dapat diterapkan secara lebih luas dalam industri keuangan.

Studi Kasus Praktis

Studi kasus yang diambil dari implementasi blockchain di beberapa layanan fintech dan bank digital menunjukkan bahwa penerapan blockchain telah berhasil meningkatkan sistem keamanan data mereka. Sebagai contoh, beberapa platform fintech telah menggunakan blockchain untuk mencatat transaksi dan mengamankan data pribadi pengguna, memastikan bahwa data tersebut tidak dapat dimodifikasi atau diakses oleh pihak yang tidak berwenang. Selain itu, beberapa bank besar juga mulai mengadopsi teknologi ini untuk memperkuat sistem transaksi mereka, terutama dalam hal verifikasi identitas dan pengelolaan data klien. Meskipun ada tantangan dalam adopsi awal, hasil yang diperoleh menunjukkan bahwa blockchain memiliki potensi besar untuk meningkatkan keandalan dan keamanan sistem keuangan secara keseluruhan.

Dalam implementasi sistem berbasis blockchain dan potensi integrasi AI-IoT, perhatian terhadap privasi dan etika menjadi krusial. Sistem dirancang mengikuti prinsip Privacy-by-Design, dengan enkripsi end-to-end dan pemisahan identitas pengguna. Sistem juga dilengkapi framework tata kelola data yang mengacu pada standar GDPR dan regulasi OJK. Implikasi seperti bias algoritma, akses terhadap data publik, dan transparansi sistem menjadi bagian dari pertimbangan desain sistem yang direkomendasikan.

4. KESIMPULAN

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, dapat disimpulkan bahwa teknologi blockchain dapat secara efektif meningkatkan keamanan data di industri keuangan dengan menyediakan sistem yang terdesentralisasi, transparan, dan tahan terhadap manipulasi. Implementasi blockchain memberikan manfaat signifikan dalam hal integritas data, audit trail, dan resistensi terhadap serangan cyber. Sistem yang dikembangkan menggunakan SDLC model waterfall dengan pemodelan UML terbukti dapat menghasilkan solusi keamanan yang robust dan dapat diandalkan.

Pengujian blackbox menunjukkan bahwa semua fungsi sistem bekerja sesuai dengan spesifikasi dan memenuhi persyaratan keamanan yang ditetapkan. Meskipun menghadapi tantangan dalam hal skalabilitas dan biaya implementasi, potensi blockchain untuk mentransformasi keamanan data di

industri keuangan sangat menjanjikan. Penelitian ini memberikan kontribusi penting dalam memahami implementasi praktis teknologi blockchain untuk keamanan data dan dapat menjadi referensi bagi lembaga keuangan yang ingin mengadopsi teknologi ini.

Saran untuk penelitian selanjutnya adalah mengeksplorasi optimisasi skalabilitas blockchain, analisis cost-benefit jangka panjang, dan pengembangan framework regulasi yang mendukung adopsi blockchain dalam industri keuangan.

DAFTAR PUSTAKA

- [1] M. A. Afif, V. Verry, and M. N. Dasaprawira, "Strategi Pengembangan Technopreneurship Berbasis Teknologi Blockchain Dalam Industri Keuangan," *JUSIM (Jurnal Sist. Inf. Musirawas)*, vol. 9, no. 1, pp. 15–22, Jun. 2024, doi: 10.32767/JUSIM.V9I1.2249.
- [2] W. Fitri, "Kajian Penerapan Smart Contract Syariah dalam Blockchain: Peluang dan Tantangan," *JATISWARA*, vol. 38, no. 2, pp. 223–232, Jul. 2023, doi: 10.29303/JTSW.V38I2.526.
- [3] Djumadi, "Teknologi Blockchain dalam Perspektif Ekonomi Islam / Keuangan Islam," *Al-Kharaj J. Ekon. Keuang. Bisnis Syariah*, vol. 6, no. 4, pp. 4335–4351, Feb. 2024, doi: 10.47467/ALKHARAJ.V6I4.887.
- [4] A. Arwani and U. Priyadi, "Eksplorasi Peran Teknologi Blockchain dalam Meningkatkan Transparansi dan Akuntabilitas dalam Keuangan Islam: Tinjauan Sistematis," *J. Ekon. BISNIS DAN Manaj.*, vol. 2, no. 2, pp. 23–37, Mar. 2024, doi: 10.59024/JISE.V2I2.653.
- [5] M. Masnur and A. Asra, "Sistem Informasi E-Farming Berbasis Web Di Kabupaten Pinrang," *J. Sintaks Log.*, vol. 1, no. 3, pp. 166–171, Oct. 2021, doi: 10.31850/JSILOG.V1I3.1111.
- [6] I. A. Rista, "Analisis Implementasi Teknologi Blockchain dalam Meningkatkan Transparansi, Efisiensi, dan Keamanan Transaksi Keuangan Perbankan Syariah Indonesia," *J. Huk. Ekon. Syariah AICONOMIA*, vol. 3, no. 2, pp. 92–106, Dec. 2024, doi: 10.32939/ACM.V3I2.4575.
- [7] H. Hatma, M. N. Akbar, and M. Masnur, "Sistem Database Terdistribusi Dalam Implementasi e-Government Pada Dinas Pencatatan Sipil Kab. Pangkep," *J. Syst. Comput. Eng.*, vol. 4, no. 1, pp. 82–91, Jan. 2023, doi: 10.47650/JSCE.V4I1.715.
- [8] imam kharits najibulloh and leny rahmalia, "Penerapan Teknologi Blockchain Dalam Industri Keuangan Syariah : Tantangan Dan Peluang," *J-EBI J. Ekon. Bisnis Islam*, vol. 3, no. 01, Mar. 2024, doi: 10.57210/J-EBI.V3I01.295.
- [9] M. F. Putranto, P. Zulfikar, M. Kamil, and H. Aziz, "Analisis Penerapan Blockchain Dalam Penyelenggaraan Administrasi Pemerintahan Dan Keuangan Negara Untuk Meningkatkan Kepastian Dan Kepatuhan Hukum: Studi Kasus Di Estonia," *J. PEMANDHU*, vol. 5, no. 2, pp. 103–119, 2024, Accessed: Jun. 14, 2025. [Online]. Available: <https://ejournal.unis.ac.id/index.php/JM/article/view/6556>.
- [10] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55-81.
- [11] Suendri. (2018). Implementasi diagram UML (Unified Modelling Language) pada perancangan sistem informasi. *Jurnal Ilmu Komputer dan Informatika*, 3(1), 1-8.
- [12] Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media.
- [13] Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world*. Portfolio.
- [14] Wahid, A. A. (2020). Analisis metode waterfall untuk pengembangan sistem informasi. *Jurnal Ilmu-ilmu Informatika dan Manajemen STMIK*, 2(1), 23-32.
- [15] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. *PLoS ONE*, 11(10), e0163477.
- [16] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *IEEE 6th International Congress on Big Data*, 557-564.
- [17] Zhao, G., Liu, S., Lopez, C., Lu, H., Elgueta, S., Chen, H., & Boshkoska, B. M. (2019). Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions. *Computers in Industry*, 109, 83-99.
- [18] Zhang, P., & Schmidt, D. C. (2020). Blockchain applications and challenges in cybersecurity. *IEEE Security & Privacy*, 18(4), 34-42.

- [19] Kim, S. K., & Huh, J. H. (2018). A study on the improvement of smart grid security performance and blockchain smart grid perspective. *Energies*, 11(8), 1973.
- [20] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*, 107, 841-853.
- [21] Yuan, Y., & Wang, F. Y. (2016). Towards blockchain-based intelligent transportation systems. *IEEE Conference on Intelligent Transportation Systems*, 2663-2668.