e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Blockchain Approach As A Digital Identity Security Solution In Banking Digital Transformation

Umar Al Faruq Siregar [1)]; Yessi Claudia Sitepu [2)]; Mawar Adelia Br Marpaung [3)]; Samuel Rizky Ananda Sitindaon [4)]; Fadly Robbani Tua Lumban Tobing [5)]; Sudarto [6]

[1,2,3,4,5,,6)]Department of Information Systems, Universitas Mikroskil Medan

Email: [1)] Umaraf204@gmail.com ;[2)] diaayessi@gmail.com ;[3)] mawaradeliamarpaung05@gmail.com
[4)] samuelrizky336@gmail.com ;[5)] fadlytobing16@gmail.com ;[6)] sudarto@mikroskil.ac.id

How to Cite :

Siregar, U. A. F., Sitepu, Y. C., Marpaung, M. A. B., Sitindaon, S. R. A., Tobing, F. R. T. L., Sudarto. (2026). Blockchain Approach As A Digital Identity Security Solution In Banking Digital Transformation. Jurnal Media Computer Science, 5(1).

ARTICLE HISTORY

Received [10 Desember 2025]
Revised [08 Januari 2026]
Accepted [15 Januari 2026]

KEYWORDS

Blockchain, Digital Identity, Data Security, Digital Transformation, Banking, Systematic Literature Review (SLR).

ABSTRAK

Transformasi digital di sektor perbankan menuntut peningkatan keamanan dalam pengelolaan identitas digital nasabah. Sistem terpusat yang umum digunakan masih rentan terhadap pencurian data, penipuan identitas, dan serangan siber, sehingga diperlukan pendekatan yang lebih aman dan terdesentralisasi. Penelitian ini bertujuan untuk mengkaji pemanfaatan teknologi blockchain dalam meningkatkan keamanan identitas digital pada perbankan digital menggunakan metode Systematic Literature Review (SLR). Metode ini dilakukan melalui pemilihan dan analisis artikel ilmiah yang relevan untuk mengidentifikasi tren, tantangan, dan efektivitas penerapan blockchain. Hasil penelitian menunjukkan bahwa blockchain mampu meningkatkan keandalan data identitas digital melalui mekanisme kriptografi, sistem desentralisasi, serta proses verifikasi tanpa pihak ketiga. Penerapan smart contract dan Decentralized Identifiers (DID) juga memperkuat proses autentikasi dan mengurangi risiko penipuan. Oleh karena itu, blockchain berpotensi menjadi fondasi penting dalam membangun sistem perbankan digital yang aman, transparan, dan terpercaya, meskipun masih memerlukan dukungan regulasi dan kesiapan infrastruktur agar dapat diterapkan secara optimal.

ABSTRACT

Digital transformation in the banking sector requires stronger security in managing customers' digital identities. Conventional centralized systems remain vulnerable to data breaches, identity fraud, and cyberattacks, highlighting the need for a more secure and decentralized approach. This study aims to examine the use of blockchain technology as an alternative solution to enhance digital identity security in digital banking systems using the Systematic Literature Review (SLR) method. This approach involves selecting and analyzing relevant scholarly articles to identify trends, challenges, and the effectiveness of blockchain implementation. The findings indicate that blockchain can improve the reliability and accuracy of digital identity data through cryptographic mechanisms, decentralized systems, and verification processes that do not rely on third parties. In addition, the use of smart contracts and Decentralized Identifiers (DID) strengthens authentication processes and reduces the risk of fraud. Therefore, blockchain has the potential to become a key foundation for building a secure, transparent, and trustworthy digital banking ecosystem, although clear regulations and adequate infrastructure readiness are still required for optimal implementation.

PENDAHULUAN

Transformasi digital di industri perbankan telah menghasilkan perubahan signifikan pada layanan keuangan yang semakin bergantung pada teknologi. Inovasi seperti perbankan digital, dompet elektronik, dan transaksi daring memberikan kemudahan serta efisiensi luar biasa bagi para pengguna. Namun, kemajuan ini juga memberikan tantangan baru, terutama soal keamanan data dan perlindungan identitas digital pelanggan. Ancaman seperti pencurian informasi pribadi, penyalahgunaan identitas, serta serangan siber yang menargetkan sistem perbankan digital menunjukkan bahwa mekanisme keamanan tradisional yang berbasis pusat masih memiliki banyak kelemahan. Situasi ini mendorong perlunya sistem keamanan yang lebih kuat, jelas, dan sulit diubah sesuka hati orang lain[1].

Teknologi blockchain muncul sebagai inovasi potensial untuk mengatasi masalah tersebut. Blockchain adalah sistem pencatatan digital terdistribusi yang beroperasi tanpa otoritas pusat, di mana setiap transaksi dicatat dalam blok-blok yang saling terhubung dengan mekanisme enkripsi kriptografi. Proses verifikasi dilakukan secara bersama-sama oleh seluruh jaringan pengguna, sehingga perubahan pada blok hampir tidak mungkin dilakukan tanpa persetujuan kolektif. Mekanisme ini memberikan keunggulan blockchain dalam menjaga integritas, kerahasiaan, dan ketersediaan data. Teknologi ini juga dikenal karena transparansi dan keandalannya yang tinggi dalam mengamankan data, serta kemampuannya mengurangi ketergantungan pada pihak ketiga untuk verifikasi informasi[2][3].

Berbagai studi menunjukkan bahwa blockchain dapat meningkatkan keamanan data digital secara substansial. Penerapan smart contract berbasis blockchain telah terbukti memperkuat autentikasi transaksi dan integritas data melalui enkripsi yang rumit[4]. Dalam bidang keuangan, penerapan teknologi ini mampu memperbaiki efisiensi operasional sekaligus memperkuat kepercayaan nasabah terhadap layanan perbankan digital[5]. Selain itu, smart contract membuka peluang untuk otomatisasi transaksi yang aman dan transparan tanpa campur tangan pihak eksternal. Pendekatan ini sejalan dengan tuntutan industri perbankan untuk sistem keuangan yang efisien, transparan, dan bebas dari risiko manipulasi[6].

Penerapan blockchain juga telah terbukti efektif di berbagai bidang lain seperti rantai pasok, ekonomi digital, dan sistem identifikasi. Teknologi ini mampu meningkatkan transparansi, kemampuan pelacakan data, serta meminimalkan risiko pemalsuan dan kebocoran informasi[7]. Prinsip-prinsip ini dapat diterapkan pada sistem keamanan identitas digital perbankan untuk memperkuat keandalan proses autentikasi pengguna. Dengan pendekatan ini, pengelolaan identitas digital dapat beralih dari model sentral ke desentralisasi yang memberikan kontrol penuh kepada individu atas data pribadinya. Konsep ini disebut self-sovereign identity, di mana pengguna memiliki kewenangan utuh untuk mengatur akses ke informasi pribadi mereka secara aman dan terenkripsi[8].

METODE PENELITIAN

Metode Pengumpulan Data

Metode pengumpulan data dalam penelitian ini menggunakan Systematic Literature Review (SLR), yaitu cara yang terorganisasi dan rapi untuk mencari, mengevaluasi, sertka menyimpulkan hasil penelitian sebelumnya mengenai penerapan teknologi blockchain di bidang perbankan. Penelitian ini berfokus pada analisis data secara kuantitatif yang berasal dari berbagai jurnal ilmiah yang sudah diterbitkan. Data dikumpulkan dengan mencari literatur di platform akademik seperti Google Scholar menggunakan kata kunci seperti blockchain technology, banking security, dan digital transformation in finance.Pemilihan artikel dibatasi pada periode tahun 2021 hingga 2025 agar data yang didapatkan tetap relevan dan sesuai dengan perkembangan teknologi terbaru. Kriteria pemilihan artikel mencakup jurnal yang terindeks Sinta atau memiliki reputasi akademik yang baik untuk menjamin kualitas dan keaslian sumber data. Setiap artikel yang terpilih dianalisis dengan

pendekatan content analysis, dengan tujuan untuk menemukan tren, manfaat, tantangan, dan peluang dalam penerapan blockchain dalam meningkatkan keamanan data di sektor perbankan.

Tahapan Penelitian

Tahapan dalam penelitian ini meliputi beberapa langkah utama, yaitu:

1. Mengidentifikasi masalah dan tujuan penelitian agar mengetahui fokus serta arah dari studi literatur.
2. Melakukan pencarian artikel terkait penerapan blockchain di bidang perbankan melalui database ilmiah.
3. Memilih artikel yang relevan berdasarkan tahun terbit, indeksasi, serta keterkaitannya dengan topik penelitian.
4. Menganalisis isi artikel yang dipilih untuk menemukan pola serta temuan inti.
5. Menyusun hasil dan pembahasan berdasarkan penyederhanaan dan penggabungan data dari artikel yang telah dianalisis.

HASIL DAN PEMBAHASAN

Blockchain adalah salah satu inovasi digital yang memberikan perubahan besar di bidang teknologi informasi. Teknologi ini bekerja sebagai sistem yang mengelola transaksi dan data secara terdesentralisasi, pertama kali diperkenalkan melalui cryptocurrency Bitcoin oleh seseorang bernama Satoshi Nakamoto. Kata *blockchain* sering dikaitkan dengan teknologi buku besar terdistribusi (DLT), yaitu sistem catatan digital yang tersimpan di berbagai titik dalam jaringan dan bisa mencatat setiap transaksi secara permanen serta tidak bisa diubah. Setiap transaksi dimasukkan ke dalam blok yang saling terhubung dengan menggunakan algoritma kriptografi, membentuk sebuah rantai blok yang sulit untuk diubah atau dimanipulasi. Dengan sifat utama seperti keamanan yang tinggi, transparansi, desentralisasi, dan kemampuan audit yang baik, blockchain mampu menciptakan kepercayaan baru dalam sistem digital yang sebelumnya bergantung pada satu pihak saja[9].

Teknologi *blockchain* kini jadi perhatian di seluruh dunia karena bisa mencatat transaksi dengan aman tanpa perlu bantuan pihak ketiga. Awalnya dibuat untuk menukar uang digital, sekarang teknologi ini berkembang dan digunakan di berbagai bidang, seperti akuntansi dan perbankan. Dalam sistem akuntansi, blockchain ternyata bisa melindungi data lebih baik, memperkuat kejujuran laporan keuangan, dan mengurangi biaya administrasi. Fitur transparansi yang dimilikinya memudahkan auditor dan lembaga keuangan untuk memeriksa transaksi secara langsung, sehingga proses keuangan jadi lebih efisien dan akurat[10].

Dari sisi keamanan, blockchain dilengkapi dengan berbagai lapisan teknologi seperti hash function, rantai hash, enkripsi kunci publik–privat, serta jaringan Peer to Peer (P2P). Lapisan-lapisan ini bekerja sama untuk memastikan integritas dan keaslian setiap data yang tersimpan di dalam sistem. Desain seperti ini menjadikan blockchain sangat cocok digunakan untuk pengelolaan data publik yang sensitif, termasuk identitas digital nasabah perbankan.

Dalam proses transformasi digital di sektor perbankan, keamanan identitas digital sangat penting. Sistem identitas yang terpusat rentan terhadap pencurian data, penipuan, dan akses yang tidak sah. Blockchain menjadi solusi yang lebih baik untuk mengatasi masalah tersebut. Karena sifatnya yang terdistribusi, terbuka, dan menerapkan enkripsi yang tangguh, blockchain bisa menciptakan sistem identitas yang lebih aman, dapat diandalkan, dan sulit dipalsukan[9]. Data identitas pelanggan disimpan dalam blok-blok yang terenkripsi dan saling terhubung. Jika ada perubahan pada satu blok, maka seluruh rantai blok akan terpengaruh. Hal ini membantu menjaga integritas dan keaslian data pelanggan secara keseluruhan..

Dalam penerapannya, proses validasi identitas seperti Know Your Customer (KYC) atau autentikasi saat login dapat dilakukan secara otomatis oleh jaringan node melalui mekanisme konsensus. Berbeda dengan sistem tradisional yang menggunakan satu server pusat, setiap node

dalam jaringan blockchain ikut serta secara aktif dalam proses pemeriksaan tersebut. Cara kerja ini sangat efektif dalam mengurangi kemungkinan terjadi gangguan sistem dan kebocoran data. Selain itu, menggunakan smart contract memungkinkan pemeriksaan identitas dilakukan secara otomatis tanpa perlunya campur tangan manusia, sehingga lebih menghemat waktu dan biaya. Semua aktivitas yang terjadi dicatat secara permanen dan bisa diperiksa kapan saja, sehingga memperkuat kepercayaan antara bank dan nasabah serta mendukung terbentuknya sistem perbankan yang modern, efisien, dan memiliki integritas tinggi[1].

Teknologi blockchain juga mendukung prinsip anonimitas dan privasi pengguna. Identitas nasabah tidak disimpan dalam bentuk data mentah, melainkan dalam bentuk yang terenkripsi, sehingga hanya bisa diakses oleh pihak berwenang. Setiap transaksi yang masuk ke dalam jaringan blockchain diubah menjadi sebuah hash unik yang tidak bisa diubah lagi atau dihapus. Hal ini membantu mencegah penipuan identitas dan memastikan data nasabah tetap valid dalam setiap transaksi digital. Jika satu node mengalami masalah, data tetap bisa diakses melalui node lainnya tanpa kehilangan keaslian, karena sifat desentralisasi dari blockchain. Melalui mekanisme tersebut, blockchain tidak hanya memberikan peningkatan pada aspek keamanan dan privasi, tetapi juga mendukung terciptanya efisiensi serta keandalan yang lebih kuat dalam sistem perbankan digital. [11].

Melalui metode Systematic Literature Review (SLR), penelitian ini mengungkap bahwa teknologi blockchain memiliki potensi signifikan dalam memperkuat keamanan identitas digital pada sektor perbankan. Sistem keuangan yang sekarang ini bergantung pada mekanisme berpusat biasanya lebih mudah terserang oleh serangan siber dan penipuan identitas. Dengan catatan transaksi yang dienkripsi dan disimpan secara terdistribusi, blockchain dapat mengurangi risiko perubahan data secara signifikan[12].

Model implementasi yang sering digunakan di bidang perbankan adalah blockchain yang bersifat permissioned atau consortium blockchain. Dalam sistem ini, beberapa lembaga keuangan bekerja sama untuk mengelola jaringan bersama yang digunakan dalam proses memverifikasi identitas nasabah. Sistem ini umumnya menggunakan komponen seperti Decentralized Identifiers (DID) dan Verifiable Credentials (VC) yang mengacu pada standar W3C, sehingga memungkinkan kerja sama dan kompatibilitas antar lembaga[12]. Selain itu, berbagai penelitian juga menyarankan penggunaan teknologi kriptografi canggih seperti Zero-Knowledge Proofs (ZKP) dan selective disclosure, yang memungkinkan pihak terkait memverifikasi identitas seseorang tanpa harus mengungkapkan seluruh informasi pribadinya[13].

Namun, penggunaan blockchain di Indonesia masih menghadapi beberapa tantangan. Hasil penelitian menunjukkan bahwa hambatan utama terdiri dari kurangnya pemahaman pegawai tentang prinsip akurat, keterbatasan dalam infrastruktur digital, rendahnya tingkat keamanan siber, serta belum adanya aturan yang jelas mengenai penggunaan blockchain. Partisipasi masyarakat dalam pengawasan keuangan dan penelusuran hasil audit juga masih rendah. Untuk mengatasi masalah ini, diperlukan pelatihan bagi tenaga ahli, pembuatan peraturan yang sesuai, serta peningkatan infrastruktur digital agar penggunaan blockchain di sektor keuangan dan publik dapat berjalan efektif dan berkelanjutan[14].

Blockchain memiliki kemampuan besar untuk meningkatkan efisiensi, keamanan, dan transparansi dalam sistem keuangan. Dengan menggunakan mekanisme desentralisasi, hashing, serta algoritma konsensus, blockchain dapat memastikan bahwa setiap transaksi valid tanpa harus melibatkan pihak ketiga. Dalam bidang perbankan, penggunaan teknologi ini memungkinkan proses pembayaran antar negara berjalan lebih cepat, biaya operasional turun, serta audit bisa dilakukan secara langsung dan real-time. Selain itu, smart contract juga membantu mengotomatisasi berbagai layanan seperti pinjaman, deposito, dan pembayaran bunga. Dengan demikian, blockchain memiliki potensi besar untuk menjadi dasar utama dalam transformasi digital perbankan Indonesia menuju sistem keuangan yang lebih aman, transparan, dan kompetitif secara internasional[15][16].

e-ISSN 2828-0490
JURNAL
MEDIA COMPUTER SCIENCE

Pendekatan berbasis blockchain dalam menjaga keamanan identitas digital bisa dilakukan dengan beberapa cara, seperti Self-Sovereign Identity (SSI), Decentralized Identifiers (DID), dan Verifiable Credentials (VC). SSI memungkinkan pengguna mengontrol semua data identitas mereka sepenuhnya, sementara DID dan VC memudahkan proses memverifikasi identitas secara terdesentralisasi dengan kunci publik dan privat yang berbeda. Cara ini sangat efektif dalam mengurangi risiko palsu dan kebocoran informasi pribadi.

Dari sisi keamanan kriptografi, sejarah perkembangan kriptografi terbagi menjadi tiga periode:

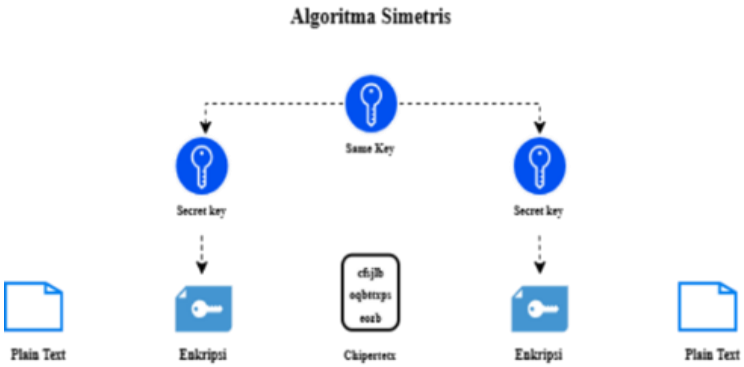
Kriptografi Klasik

Pada periode tersebut, teknik enkripsi diklasifikasikan ke dalam dua kategori utama, yakni algoritma transposisi dan algoritma substitusi. Kriptografi klasik yang digunakan sebelum dan setelah komputer ditemukan tidak disarankan untuk melindungi informasi penting karena mudah dibobol. Metode ini hanya mengacak huruf A-Z dengan menggunakan karakter sebagai dasarnya, dan cara kerjanya adalah dengan menggunakan pena serta kertas. Salah satu contoh algoritma substitusi adalah Caesar Cipher, yang pertama kali digunakan saat Yulius Caesar memimpin pemerintahan.

Kriptografi Modern

Kriptografi modern adalah jenis kriptografi yang cukup rumit. Untuk menguasainya, diperlukan pemahaman tentang matematika. Karena itu, kriptografi modern berkembang seiring perkembangan komputer hingga masa kini. Kriptografi modern terdiri dari tiga bagian, yaitu:

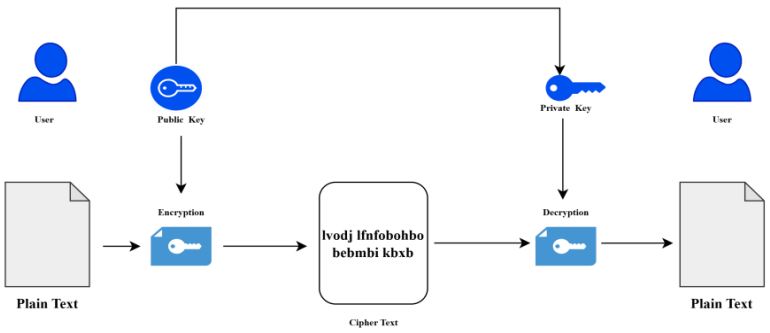
1) Algoritma Simetris



Gambar 1. Algoritma Simetris

Berdasarkan pada Gambar 1, algoritma simetris bekerja dengan memakai kunci yang identik untuk proses enkripsi maupun dekripsi data. Algoritma kriptografi jenis ini dikenal juga sebagai algoritma kunci rahasia, kunci tunggal, atau satu kunci. Agar dapat digunakan, pengirim dan penerima harus terlebih dahulu menyetujui penggunaan kunci yang sama.

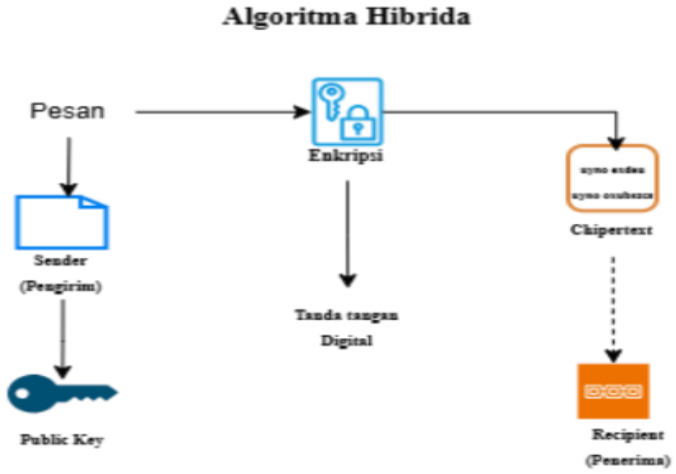
2) Algoritma Asimetris



Gambar 2. Algoritma Asimetris

Berdasarkan pada Gambar 2, algoritma asimetris merupakan teknik kriptografi yang memanfaatkan sepasang kunci. Satu kunci dipakai dalam proses enkripsi maupun dekripsi. Siapa pun yang memiliki kunci publik dapat menggunakannya untuk mengenkripsi pesan, sedangkan hanya pemilik kunci privat yang berhak membuka atau mendekripsi pesan tersebut.

3) Algoritma Hibrida



Gambar 3. Algoritma Hibrida

Berdasarkan pada Gambar 1.3, algoritma hibrida memanfaatkan dua tipe kunci, yakni kunci rahasia atau kunci simetris sering disebut juga kunci sesi untuk proses enkripsi data, serta pasangan kunci publik dan kunci privat yang berfungsi dalam pembuatan tanda tangan digital sekaligus melindungi kunci simetris.

Kriptografi Kontemporer

Periode ini berfokus pada penerapan algoritma modern yang kompleks dalam sistem nyata untuk mencapai keamanan data yang berlapis-lapis, contohnya:

1. Penerapan algoritma RSA dalam sistem informasi perpustakaan untuk melindungi kerahasiaan data.
2. Penggunaan AES (AES-128, 192, dan 256 bits) untuk mengamankan pesan teks, konten dokumen, dan file dokumen.
3. Kombinasi antara kriptografi (seperti AES), dan steganografi, yaitu teknik menyembunyikan pesan dalam media lain seperti gambar, untuk melindungi data dengan cara yang lebih canggih dan sangat rahasia. Saat ini, kriptografi tidak hanya digunakan untuk mengkodekan data, tetapi juga berkembang dalam berbagai hal seperti enkripsi dan dekripsi, autentikasi, tanda tangan digital, protokol pertukaran kunci, uang digital, dan masih banyak lagi [17].

Dari sisi teknis, hashing merupakan komponen penting dalam sistem blockchain, di mana data diubah menjadi kode unik dengan panjang tetap dan tidak dapat dikembalikan ke bentuk aslinya. Mekanisme ini memungkinkan setiap perubahan data dapat terdeteksi. Selain itu, jaringan Peer to Peer (P2P) memungkinkan setiap node berperan dalam proses verifikasi, sehingga setiap transaksi harus divalidasi sebelum ditambahkan ke dalam blok.

Meskipun memiliki berbagai keunggulan, blockchain masih menghadapi kendala, terutama terkait kompatibilitas antar sistem karena belum adanya standar umum yang mengatur interoperabilitas. Selain itu, sifat data yang tidak dapat diubah menyulitkan proses penghapusan atau perbaikan informasi. Namun, melalui pengembangan teknologi terbuka dan kerja sama antar lembaga, kendala tersebut dapat diatasi secara bertahap.

Secara umum, penerapan blockchain dalam transformasi digital perbankan berpotensi meningkatkan keamanan identitas digital, mempercepat proses transaksi, dan meningkatkan kepercayaan masyarakat terhadap sistem keuangan digital. Dengan dukungan regulasi yang jelas, kesiapan infrastruktur, serta peningkatan pemahaman teknologi, blockchain dapat menjadi fondasi penting dalam membangun sistem perbankan yang aman, transparan, dan berkelanjutan di era digital

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil pembahasan, teknologi blockchain memiliki potensi besar dalam meningkatkan keamanan identitas digital pada sektor perbankan. Sifat blockchain yang tidak terpusat, transparan, serta didukung oleh mekanisme enkripsi seperti hash function dan kriptografi kunci publik dan privat mampu menjaga integritas dan keaslian data nasabah. Selain itu, penerapan konsep Self-Sovereign Identity (SSI), Decentralized Identifiers (DID), dan Verifiable Credentials (VC) memungkinkan nasabah mengelola data pribadi secara mandiri. Penggunaan smart contract dan mekanisme konsensus juga memungkinkan proses verifikasi identitas dilakukan secara otomatis, efisien, dan aman tanpa keterlibatan pihak ketiga, sehingga meningkatkan kepercayaan, transparansi, dan efisiensi operasional sistem keuangan digital.

Namun, penerapan blockchain di sektor perbankan masih menghadapi beberapa kendala, antara lain keterbatasan infrastruktur digital, belum optimalnya regulasi, rendahnya pemahaman sumber daya manusia, serta masalah kompatibilitas antar sistem dan pembaruan data. Oleh karena itu, pengembangan blockchain di Indonesia memerlukan dukungan kebijakan pemerintah, peningkatan literasi teknologi, serta kolaborasi antar lembaga keuangan melalui consortium blockchain. Dengan upaya tersebut, blockchain berpotensi menjadi fondasi sistem perbankan digital yang aman, efisien, dan terpercaya.

Saran

Berdasarkan hasil penelitian, pemerintah dan regulator perbankan diharapkan dapat menyusun regulasi yang jelas dan mendukung penerapan teknologi blockchain, khususnya dalam pengelolaan identitas digital, agar memberikan kepastian hukum bagi lembaga perbankan. Selain itu, pihak perbankan disarankan untuk mulai menerapkan teknologi blockchain secara bertahap melalui kerja sama antar bank dalam bentuk consortium blockchain guna meningkatkan keamanan data, efisiensi operasional, dan interoperabilitas sistem.

Selanjutnya, peningkatan pemahaman dan keterampilan sumber daya manusia terkait teknologi blockchain, termasuk konsep SSI, DID, dan VC, perlu menjadi perhatian utama agar implementasi dapat berjalan optimal. Bagi penelitian selanjutnya, disarankan untuk melakukan kajian empiris mengenai penerapan blockchain pada sistem identitas digital perbankan di Indonesia, termasuk kesiapan infrastruktur dan penerimaan pengguna, sehingga dapat memberikan gambaran yang lebih komprehensif. Dengan dukungan regulasi, SDM yang kompeten, serta kolaborasi antar lembaga, teknologi blockchain berpotensi menjadi fondasi sistem perbankan digital yang aman dan terpercaya.

DAFTAR PUSTAKA

S. Afdilah, N. S. Agustina, I. Hani, and G. Gunawan, “Penerapan Teknologi Blockchain dalam Meningkatkan Keamanan Sistem Identifikasi Pengguna,” J. Software, Hardw. Inf. Technol., vol. 4, no. 2, pp. 47–62, 2024, doi: 10.24252/shift.v4i2.142.

D. Yudih, Iqlima, M. Ridwan, and A. Nursiwan, “Penggunaan Teknologi Blockchain dalam Perbankan,” El-Ecosy J. Ekon. dan Keuang. Islam, vol. 4, no. 2, pp. 145–155, 2024, doi: 10.35194/eeki.v4i2.

C. A. Ismayanti and P. H. Rantelinggi, “Simulasi Penggunaan Blockchain Pada Keamanan Jaringan Internet Of Things Menggunakan Pin Emulator: Model Public Blockchain,” J. Teknol. Inf. dan Ilmu Komput., vol. 11, no. 2, pp. 235–242, 2024, doi: 10.25126/jtiik.20241126108.

R. P. Purba, B. A. Wijaya, L. W. Nazara, S. S. Utami, and D. Indonesia, “Desain Protokol Keamanan Data Berbasis Blockchain pada Pengolahan Data Pengguna Aplikasi E-commerce dapat diterapkan dalam pengolahan data untuk mengetahui desain protokol keaman Studi Literatur : Pengumpulan informasi teoritis dan penelitian terdahulu .,” Metik J., vol. 9, no. 2, pp. 256–263, 2025, doi: 10.47002/metik.v9i2.1104.

S. A. Wirayuda et al., “Penerapan teknologi blockchain berbasis smart contract untuk meningkatkan keamanan transaksi finansial online,” J. SimanteC, vol. 14, no. 1, pp. 11–20, 2025, doi: 10.21107/simantec.v14i1.

W. Fitri, “Kajian Penerapan Smart Contract Syariah dalam Blockchain: Peluang dan Tantangan,” Jatiswara, vol. 38, no. 2, pp. 223–232, 2023, doi: 10.29303/jtsw.v38i2.526.

H. C. W. A, M. A. R. B, B. S. A, and I. G. C. Marco, “Blockchain dalam Rantai Pasokan Pangan : Tinjauan Literatur dan Analisis Bibliometrik,” SPEKTRUM Ind., vol. 23, no. 1, pp. 42–57, 2025, doi: 10.12928.

Riki Renaldo and Kbina Buono, “Blockchain dalam Ekonomi Sistem Informasi sebagai upaya Meningkatkan Transparansi dan Kepercayaan dalam Transaksi Digital di Kota Agung Kabupaten Tanggamus Lampung,” J. Ekon. Manaj. Sist. Inf., vol. 6, no. 4, pp. 2461–2470, 2025, doi: 10.38035/jemsi.v6i4.4558

Arnadi Chairunnas, Efendi Sugianto, Rina Pratiwi, Michael Sitorus, and Bambang Cahyono, “Teknologi Blockchain dalam Transformasi Keuangan dan Perbankan: Potensi dan Tantangan,” J. Econ. Educ. Entrep. Stud., vol. 5, no. 2, pp. 279–290, 2024, doi: 10.62794/je3s.v5i2.3568z

F. V. Palidita, W. T. Suci, and Z. Azmi, “PENGGUNAAN TEKNOLOGI BLOCKCHAIN DALAM SISTEM INFORMASI AKUNTANSI : PELUANG DAN TANTANGAN,” J. Akunt. Akt., vol. 5, no. 1, pp. 39–45, 2024, doi: 10.21009/jpepa.0501

F. Felicia, E. Elvilie, C. Calista, S. A. Chic, M. F. Bilqisthi, and J. Joosten, “Tantangan dan Peluang Blockchain di Era Digital dalam Bidang Keamanan Data dan Transaksi Digital,” J. Compr. Sci., vol. 3, no. 11, pp. 5131–5147, Dec. 2024, doi: 10.59188/jcs.v3i11.2887.

A. Munandar, Nurul Huda, and Nafisah Nurulrahmatiah, “Pengaruh Teknologi Blockchain terhadap Kepercayaan dan Efisiensi Transaksi di Sektor Perbankan,” J. Publ. Manaj. Inform., vol. 4, no. 1, pp. 01–17, 2024, doi: 10.55606/jupumi.v4i1.3434.

R. Kusumaningsih, “Perkembangan Legalitas Teknologi Blockchain dalam Industri Keuangan di Indonesia,” J. Ilmu Sos. Hum. Indones., vol. 5, no. 1, pp. 113–121, 2025, doi: 10.52436/1.jishi.161.

E. Pratiwi, S. Parapat, D. Siringo-Ringo, and J. Siahaan, “Kerangka Audit Real-Time Berbasis Blockchain untuk Tata Kelola Keuangan Sektor Publik di Indonesia: Studi Kasus Tantangan Implementasi IPSAS dan Reformasi Kelembagaan,” J. Mhs. Manaj. dan Akunt., vol. 4, no. 2, pp. 318–331, 2025, doi: 10.30640/jumma45.v4i1.4435.

R. Mustaqim Handoko et al., “Implementasi Blockchain Untuk Keamanan Sistem Pembayaran Digital dan Optimasi Transaksi Keuangan (Studi Kasus Industri Fintech di Indonesia),” J. Ilmu Tek. dan Inform., vol. 4, no. 2, pp. 64–74, 2024, doi: 10.51903/teknik.

S. J. H.A, G. M. D. P. Rahadi, M. Mediaty, and D. Damayanti, “Dampak Teknologi Blockchain pada Sistem Pengendalian Internal Perusahaan di Sektor Keuangan,” J-CEKI J. Cendekia Ilm., vol. 3, no. 4, pp. 964–976, 2024, doi: 10.56799/jceki.v3i4.3774.

N. Amalya, S. M. Sopiana Silalahi, D. F. Nasution, M. Sari, and I. Gunawaan, “JURNAL MEDIA INFORMATIKA [JUMIN] Kriptografi dan Penerapannya Dalam Sistem Keamanan Data,” J. Media Inform. [Jumin], vol. 4, no. 2, pp. 90–93, 2023, doi: 10.55338/jumin.