JBEP: Jurnal Bisnis, Ekonomi Syariah, dan Pajak
Volume. 1, No. 1 Maret 2024
e-ISSN :3046-9864, dan p-ISSN :3046-9880, Hal. 174-183
DOI: https://doi.org/10.61132/jbep.v1i4.738
Available online at: https://ejournal.areai.or.id/index.php/JBEP

Pemanfaatan *Blockchain* untuk Meningkatkan Keamanan Siber dalam Pembayaran Lintas Batas di Industri *Fintech*

Uky Zaza Agustiana
Prodi Ekonomi Syariah, Fakultas Ekonomi dan Bisnis Islam, UI Bunga Bangsa Cirebon, Indonesia
Korespondensi penulis : ukyzaza5@gmail.com

Abstract *The cross – border fintech payment industry faces many cybersecurity issues, including the possibility of data theft, fraud and low efficiency due to reliance on conventional intermediaries. Based on decentralized and cryptgrahpic system, blockchain technology can improve the security and efficiency of cross – border payments. The purpose of this study is to see how the implementation of blockchain affects the transparency, speed and cost of transactions. Using literature studies and case analysis, it was found that blockhain technology can reduce the risk of fraud by making institutions transparent and immutable. In addition, it allows for automated payments through smart contracats, scalability, regulation and technology adoption are some of the challenges that still hinder its implementation. The results of the study show that blockchain is an innovation strategy that has the potential to transform payments across the fintech sector, but it requires synergy between technology, policy and industry players for optimal implementation.*

Keywords: *blockchain; cybersecurity; fintech.*

Abstrak Industri fintech lintas batas pembayaran menghadapi banyak masalah keamanan siber, termasuk kemungkinan pencurian data, penipuan dan efisiensi yang rendah karena bergantung pada perantara konvensional. Teknologi berbasis pada sistem desentralisasi dan kriptografi, blockchain dapat meningkatkan keamanan dan efisiensi pembayaran lintas batas. Tujuan penelitian ini adalah untuk melihat bagaimana penerapan blockchain mempengaruhi transparasi, kecepatan, dan biaya transaksi. Dengan menggunakan studi literatur dan analisis kasus, ditemukan bahwa teknologi blockchain dapat mengurangi risiko penipuan dengan membuat lembaga transparan dan tidak dapat diubah. Selain itu, memungkinkan pembayaran otomatis melalui smart contract. Skalabilitas, regulasi, dan penerapan teknologi merupakan beberapa tantangan yang masih menghalangi pelaksanaannya. Hasil penelitian menunjukkan bahwa blockchain adalah strategi inovasi yang memiliki potensi untuk mengubah pembayaran di seluruh sektor fintech, namunperlu membutuhkan sinergi antara teknologi, kebijakan, dan pelaku industri untuk penerapan yang optimal.

Kata Kunci: *blockchain;* keamanan siber*; fintech*.

1. LATAR BELAKANG MASALAH

Dalam era digitalisasi yang semakin berkembang, industri fintech menjadi salah satu industri yang mengalami pertumbuhan pesat, terutama dalam layanan pembayaran lintas batas. Dengan pertumbuhan globalisasi perdagangan dan investasi, permintaan untuk transaksi internasional yang cepat, transparan, dan aman terus meningkat. Namun, ada sejumlah masalah di balik peluang tersebut, terutama dalam hal keamanan siber. Pencurian data, manipulasi transaksi, dan serangan malware adalah ancaman utama yang dapat membahayakan penggunaan dan bisnis fintech.

Blockchain dapat dianggap sebagai database tersebar yang berisi catatan tentang semua peristiwa digital yang telah dilakukan dan dibagikan di antara semua anggota yang berpartisipasi. Teknologi Blockchain memungkinkan jaringan peer-to-peer yang terdistribusi,

Received November 24, 2024; Revised December 08, 2024; Accepted December 22, 2024; Published December 24, 2024

di mana anggota yang saling tidak mempercayai dapat berinteraksi secara verifikasi satu sama lain tanpa otoritas yang dipercaya. (Irawan, 2023)

Sistem pembayaran lintas batas konvensional melibatkan banyak perantara, yang memperlambat proses transaksi dan meningkatkan risiko keamanan. Faktor lain yang menghambat efisiensi adalah biaya transaksi yang tinggi dan kurangnya transparasi. Dalam situasi ini, solusi kreatif diperlukan untuk mengatasi berbagai masalah yang ada. Pendekatan baru untuk mengelola transaksi keuangan ditawarkan oleh teknologi blockchain, yang berbasis pada desentalisasi.

Blockchain memiliki potensi untuk mengubah pembayaran lintas batas karena fiturnya seperti transparasi, immutability, dan keamanan melalui kriptografi. Teknologi ini memungkinkan data transaksi dicatat secara permanen dan tidak dapat diubah, sehingga mengurangi risiko penipuan dan manipulasi. Selain itu, memasukan smart contract mengurangi ketergantungan pada perantara dengan mengotomatisasi proses pembayaran. Penelitian ini bertujuan untuk menggali potensi blockchain dalam meningkatkan keamanan siber pada pembayaran lintas batas di industri fintech. Dengan memahami penerapan teknologi ini, diharapkan dapat ditemukan solusi yang mampu mengatasi tantangan keamanan sekaligus meningkatkan efisiensi dan transparasi transaksi.

Teknologi blockchain dapat di jadikan suatu transaksi lebih cepat, murah, transparan dan aman. Transaksi lebih cepat karena menggunakan platform digital sehingga transaksi jarak dekat atau jarak jauh dapat terjadi secara real time. Untuk transaksi lebih murah karena tidak membutuhkan pihak ketiga, transaksi yang lebih transparan karena setiap transaksi tercatat secara permanen dalam sistem blockchain serta dapat di verifikasi oleh pihak terkait. Dan transaksi lebih aman karena sistem verifikasi yang di distribusikan tidak dapat di hack oleh pihak manapun. (Ihsan, 2022)

2. TINJAUAN LITERATUR

Pengertian Blockchain

Blockchain adalah sistem penyimpanan transaksi digital yang terdistribusi. Sistem yang digunakan yaitu menggunakan peer to peer untuk memcatatat transaksi secara permanen dan kebenarannya. Setiap transaksi di catat dalam sebuah blok yang memungkinkan dalam sebuah urutan berantai. (Setianingsih, 2024)

Ada beberapa fitur utama dari blockchain secara signifikan dengan keamanan adalah sebagai berikut:

1. Desentralisasi: merupakan struktur sistem yang kendali atau otoritas tidak terpusat pada satu entitas tunggal atau tidak pada satuu server pusat, melainkan tersebar di beberapa jaringan, dan memastikan tidak ada satu pihak manapun yang dapat memiliki kendali penuh sehingga dalam meningkatkan keamanan, transparasi dan keandalan. Manfaatnya adalah mengurangi risiko kegagalan sistem dan meningkatkan kepercayaan karena tidak adanya otoritas tunggal dalam mengendalikan sistem.
2. Konsensus: merupakan mekanisme atau proses dalam mencapai kesepakatan bersama antara semua peserta dalam jaringan desentralisasi tentang validasi suatu transaksi. Dan digunakan pula untuk memastikan bahwa semua node dalam jaringan memiliki salinan data yang sama dan valid, sehingga terhindar dari data yang palsu. Ada beberapa metode konsensus umum yaitu a) Poor of Work (PoW), b) Poor of Stake (Pos), 3) Delegated Proof of Stake (DpoS), dan 4) Practical Byzantine Fault Tolerance (PBFT). Manfaat dari konsensus adalah untuk menghindari manipulasi data dan menjaga integritas sistem disentralisasi.
3. Enkripsi: merupakan teknik pengamanan data dengan mengubah menjadi format yang tidak dapat dibaca oleh pihak yang tidak memiliki akses tertentu yang dapat membaca data tersebut. Enkripsi dapat melindungi data transaksi, sehingga hanya pihak yang memiliki akses data tersebut yang dapat membacanya. Ada beberapa jenis enkripsi yaitu a) simetris yaitu menggunakan satu kunci untuk mendeskripsi data, dan b) asimetris yaitu menggunakan publik untuk mengenkripsi data dan privasi kunci untuk mendekripsinya. Manfaat adalah untuk menjamin kerahasiaan data dan melindungi akses dari pihak yang tidak ada berkaitannya.

Peran blockchain dalam keamanan data

Blockchain berperan sebagai solusi untuk meningkatkan keamanan melalui desentralisasi, imutabilitas dan transparasi. Teknologi ini cocok di gunakan dalam berbagai sektor seperti keuangan, kesehatan dan logistik pemerintahan untuk melindungi data dan ancaman manipulasi, pencurian dan kegagalan sistem. Potensi pada blockchain dalam keamanan data terus berkembang dengan inovasi yang sedang dilakukan.

Desentralisasi sebagai Kunci Keamanan Blockchain berbeda dengan sistem tradisional yang terpusat, di mana satu entitas memiliki kontrol penuh atas data. Dalam blockchain, data didistribusikan di seluruh jaringan, dan setiap perubahan harus disetujui oleh mayoritas node dalam jaringan. Data dalam blockchain tidak tersimpan di satu lokasi pusat melainkan

disebarluaskan, seperti apada data kesehatan yang catatan pasien di simpan pada jaringan blockchain terdistribusi sehingga lebih tahan terhadap serangan siber. Meningkatkan dalam keandalan sistem karena data tetap tersedia meskipun beberapa node mengalami kerusakan. Blockchain mencatat semua transaksi secara transparan dalam ledger publik, tetapi melindungi privasi pengguna melalui identitas anonim. Transparansi dan Integritas Data Setiap transaksi yang terjadi dalam blockchain dapat diakses oleh semua anggota jaringan, meningkatkan transparansi. Meskipun data dapat dilihat, hanya pengguna yang memiliki otoritas tertentu yang dapat melakukan perubahan, menjaga integritas data. Yang memungkinkan audit yang transparan tanpa mengungkap data sensitif pengguna dan juga mengurangi risiko penggunaan data.

Imutabilitas data , blockchain menyimpan data dalam blok yang tidak dapat dibah setelah di verfikasi. Setiap blok sebeumnya melalui kriptografi, sehingga sulit untuk memodifikasi data tanpa memengaruhi seluruh rantai. Data yang dimasukkan ke dalam blockchain biasanya sulit untuk diubah atau dihapus. Ini memberikan keamanan tambahan terhadap perubahan yang tidak sah agar mencegah dari manipulasi data dan mengurangi risiko pencurian atau penghapusan data oleh pihak yang tidak berwenang. Misalnya dalam industri keuangan transaksi di catat di blockchain untuk mencegah pengubahan data secara ilegal. Blockchain dan Keamanan dalam Transaksi Digital Blockchain dapat digunakan untuk mengamankan transaksi digital dengan memberikan cara yang lebih aman dan terverifikasi untuk mentransfer data atau uang tanpa memerlukan perantara. Aplikasi Blockchain dalam Sektor Keuangan Blockchain telah mulai diterapkan dalam sektor keuangan, dengan banyak bank yang menggunakan teknologi ini untuk meningkatkan keamanan transaksi antar bank serta untuk mengurangi biaya dan waktu transaksi.(Simanungkalit, 2024)

Smart Contracts dan Keamanan Transaksi Smart contracts adalah kontrak digital yang dijalankan secara otomatis ketika syarat-syarat tertentu terpenuhi. Ini memberikan cara yang lebih aman dan efisien untuk mengelola transaksi dan kontrak. Smart contract pada teknologi blockchain umumnya melibatkan beberapa tahapan, termasuk tahap mengidentifikasi perjanjian, menentukan kondisi, mengkodekan logika bisnis, pembaruan jaringan, pelaksanaan dan pengolahan, dan enkripsi.(Megawati et al., 2023)

3. METODOLOGI PENELITIAN

Pada penelitian ini menggunakan metode penelitian kualitatif deskriptif dengan teknik pengumpulan data yaitu studi literatur . (Suwarno, 2006) menyatakan bahwa studi literatur yaitu pengkajian data berbagai buku referensi serta hasil penelitian sebelumnya yang relevan dengan penelitian untuk mendapatkan landasan teori dari masalah yang akan diteliti. Keterbatasan ini yang hanya mengarah pada produksi artikel, jurnal dan artikel – artikel terdahulu yang setema dengan penelitian yang dibuat. Dalam penelitian ini ada beberapa teknik metode tersebut diantaranya adalah dalam menganalisis beberapa studi kasus disetiap tema yang didapatkan yaitu pada blockchain dalam keamanan siber pada fintech dari beberapa sumber yang relevan dan analisis beberapa sumber yang ada berkaitannya dengan peneitian ini.

Jenis – jenis literatur yang di gunakan yaitu primer dan sekunder. Literatur primer dalah sumber asli yang berisi data atau informasi langsung dari peneliti. Sumber ini berupa data resmi seperti studi kasus, dokemtasi dan beberapa artikel yang relevan. Literatur sekunder adalah sumber yang menginterprestasikan, meringkas atau menganalisis dari beberapa review, ulasan materi atau beberapa artikel jurnal yang di dapatkan dari beberapa analisa.

4. HASIL DAN PEMBAHASAN

Penggunaan Smart Contarct untuk Otomatisasi

Smart contract adalah program yang berjalan di atas blockchain dan bersifat self-verifying, self-executing, dan tamper - resistant. Sebuah smart contract terdiri dari sebuah nilai,, alamat, fungsi, dan state/keadaan. Input yang diterima adalah suatu transaksi, lalu kode yang berhubungan dengan transaksi tersebut, lalu memicu sebuah output. Smart contract juga dipadukan dalam melakukan transaksi. Informasi tentang barang yang dijual yang meliputi hak milik, kondisi barang, lokasi barang, dan lain-lain akan dimasukkan kedalam smart contract, beserta kondisi IFTTT (If-This-Than-That) yang harus dipenuhi sebagai bentuk dari transaksi, misalnya jumlah nominal yang harus ditransfer. (Dzakiy, 2020)

Teknologi Blockchain akhir-akhir ini telah digunakan untuk membuktikan keaslian dokumen dengan menerbitkan dokumen tersebut dalam bentuk aset digital pada jaringan publik Blockchain. Aset digital ini kemudian menjadi referensi bagi yang berkepentingan untuk memverifikasi dokumen atau salinannya dengan menggunakan QR code atau aplikasi khusus . Selain pembuktian keaslian dokumen, pelacakan juga dapat dilakukan.(Abidin et al., 2023)
Salah satu manfaat utama blockchain adalah kemampuannya untuk mengurangi biaya operasional dengan menghilangkan kebutuhan akan perantara dalam transaksi. Ini

memungkinkan perusahaan untuk mengurangi biaya yang terkait dengan verifikasi data, pemrosesan transaksi, dan administrasi, sehingga meningkatkan efisiensi operasional secara keseluruhan. Blockchain tidak hanya menjadi solusi keamanan, tetapi juga memainkan peran penting dalam transformasi digital. Dengan kemampuannya untuk mengamankan dan menyederhanakan transaksi digital, blockchain membuka jalan bagi era baru digitalisasi yang lebih aman dan efisien di berbagai sektor.

Contoh implemetasi pada smart contarct adalah NFT Blockhain-Smart Contract merupakan turunan dari teknologi aset kripto mata uang (cryptocurrency) yang sudah tentu memiliki pendekatan teknologi yang berbeda sehigga diperlukan pengetahuan baru untuk memahai mengenai tata cara dalam melakukan transaksi bisnis didalam nya sehingga dapat memahami kebasahan transaksi NFT Blockhain - Smart Contract. NFT telah dienkripsi di Blockchain Smart-Contract dan tidak bisa diduplikat, sehingga aset digital NFT sangat terjamin keasliannya. NFT juga dapat dikoleksi dan tidak bisa digandakan sehingga menjadikannya sebagai karya cipta yang langka. NFT memiliki identifikasi yang unik yang tidak dapat dipertukarkan secara langsung dengan token lain.(Fajarianto et al., 2022)

Keamanan Akses Data melalui Kriptografi

1. Algoritma Advanced Encryption Standard (AES)

   Algoritma Advanced Encryption Standard (AES) digunakan oleh sistem aplikasi untuk keamanan dokumen dan dipilih karena tingkat keamanannya yang tinggi dan pertukaran informasi yang sangat baik. Advence Encryption Standard (AES) memiliki panjang blok sebanyak 128, 192 atau 256 bit. SubBytes, ShiftRows, MixColumns, dan AddRoundKey adalah empat tipe byte transformasi yang digunakan dalam proses enkripsi AES. Input yang telah masuk ke dalam state akan mengalami perubahan AddRoundKey byte demi byte pada awal proses enkripsi. Dalam keamanan data adalah masalah kriptografi. Hal ini mencakup pembuatan proses berbasis algoritma matematika yang menyediakan sejumlah fungsi keamanan informasi utama. Karena informasi atau dokumen tersebut dapat mengandung informasi rahasia atau menjadi dokumen berharga yang perlu dirahasiakan. Salah satu cara yang dapat digunakan untuk mengamankan informasi atau dokumen adalah penggunaan sistem kriptografi.(Olivia et al., 2023)

2. Algoritma RSA

   RSA merupakan algoritma kriptografi yang menggunakan dua kunci berbeda pada proses enkripsi dan dekripsi-nya. RSA menganut sistem algoritma kunci publik yang saat ini telah digunakan secara luas. RSA pertama kali dipublikasikan pada tahun

1977. RSA merupakan metode kriptografi asimetris yang beroperasi pada mode blok. RSA membutuhkan dua kunci yang berbeda pada proses enkripsi dan dekripsi nya sehingga proses enkripsi dan dekripsi hanya dapat dilakukan oleh pihak yang memiliki kunci yang sesuai. Walaupun kunci enkripsi diketahui oleh pihak yang tidak berhak, pesan tidak dapat di dekripsi menggunakan kunci tersebut.(Syafutra & Suryana, 2022)

Proteksi dari Serangan Siber melalui Ledger Desentralisasi

1. Blockchain dan Keamanan Siber

   Blockchain mencatat transaksi secara permanen sehingga mengurangi risiko manipulasi data tanpa jejak. Ketahanan terhadap Serangan Siber: Dengan sistem yang didasarkan pada teknologi kriptografi yang kuat, blockchain dapat menjadi pertahanan yang efektif terhadap serangan siber. Struktur yang terdesentralisasi juga membuatnya lebih sulit bagi penyerang untuk mencuri atau mengganggu data. (Wardhana, 2024) Dalam keamanan siber menjadi semakin penting seiring dengan meningkatnya ketergantungan kita pada teknologi digital. Serangan siber dapat mengakibatkan kerugian finansial yang signifikan, reputasi yang rusak, dan bahkan ancaman terhadap keamanan nasional.

   Oleh karena itu, perlindungan terhadap infrastruktur digital dan data sensitif menjadi prioritas utama bagi banyak negara dan organisasi. Untuk mengatasi ancaman siber, berbagai peraturan dan regulasi telah diterapkan oleh pemerintah di seluruh dunia. Peraturan ini bertujuan untuk melindungi data pribadi, memastikan integritas sistem informasi, dan menegakkan hukum terhadap pelaku kejahatan siber. Selain itu, regulasi keamanan siber juga mendorong penerapan praktik terbaik dalam manajemen risiko dan meningkatkan kesadaran tentang pentingnya keamanan informasi. (Kristianti & Kurniasi, 2024)

2. Implementasi di Infrastruktur Penting

   Pemerintah Indonesia mengatur standar keamanan siber melalui penguatan tiga pilar arsitektur keamanan siber. Ketiga pilar arsitektur keamanan siber tersebut adalah proses (process) (berupa pengembangan kebijakan, mekanisme, tata kelola, regulasi), sumber daya manusia (people) (berupa pemberian literasi, pelatihan, seminar, atau bentuk peningkatan kapasitas lain), dan teknologi (technology) (berupa pelaksanaan riset bersama, penumbuh kembangan industri, dan lain-lain) untuk menghadapi peningkatan ancaman siber. Pemerintah indonesia melakukan beberapa strategi di antaranya yaitu pengembangan infrastruktur, kerja sama pengembangan teknologi, dan penerbitan peraturan. Strategi pertama, pengembangan infrastruktur, mencakup

pembangunan dan pemerataan infrastruktur digital. Yang kedua dengan kerjasama dengan penyelenggara telekomunikasi, baik dari dalam maupun luar negeri, sebagai bagian dari strategi pengembangan teknologi, dan terakhir adalah Pemerintah membuat kebijakan dengan memperhatikan sinergi antara aspek regulasi, spektrum frekuensi radio, model bisnis, infrastruktur, serta perangkat, ekosistem, dan talenta digital.(Vincha & Satrio, 2024)

3. Kerangka Keamanan Siber Nasional

Usaha untuk meningkatkan komitmen dunia dalam keamanan siber, dilakukan dengan pemeringkatan Global Cybersecurity Index (GCI) oleh International Telecommunication Union (ITU) kepada 193 negara-negara anggotanya. untuk mengatasi permasalahan keamanan informasi siber tidaklah mencukupi. Cybersecurity semestinya adalah sebuah ekosistem dimana hukum (laws), organisasi (organizations), kemampuan (skills), kerjasama (cooperation), dan technical implementation berjalan secara selaras untuk dapat menjadi efektif. Studi mengenai strategi keamanan siber nasional yang telah dilakukan sebelumnya menyebutkan sudah ada usaha pemerintah Indonesia untuk mengatasi meningkatnya kejahatan siber yaitu dengan strategi yang ditinjau dari lima aspek yaitu hukum, teknikal dan prosedural, struktur organisasi, peningkatan kapasitas, dan kerjasama inernasional, namun dalam implementasinya belum sesuai dengan harapan. Sedangkan studi ini bertujuan untuk memberikan gambaran tentang bagaimana strategi pemerintah dalam menghadapi tantangan keamanan siber di Indonesia saat ini dan peluang peningkatan strategi yang dapat dilakukan di masa depan dipetakan dari aspek people, process, technology.(Islami, 2017)

5. KESIMPULAN

Blockhain menawarkan transparasi dan keamanan yang lebih baik dengan sifatnya yang desentralisasi dan immutabble, yang di mana semua transaksi di catat dalam ledger publik yang tidak dapat diubah, mengurangi risiko manipulatif data dan serangan siber. Sistem berbasis blockchain mengurangi watu proses pembayaran lintas batas, teknologi blockchain dapat mengurangi biaya transaksi karena tidak ada pihak ketiga dala validasi transaksi lintas batas. Hal ini relevan untuk meningkatkan inklusi keuangan di negara berkembang.

Walaupun menfaatnya signifikan blockchain masih menghadapi tantangan, kebutuhan akan energi tinggi dalam proses mining, serta perlunya regulasi global yang seragam untuk memastikan penggunaan aman dan terstandar. Blockchain dalam industri fintech untuk pembayaran lintas batas memiliki potensi besar, tetapi keberhasilan sangat bergantung dalam regulasi yang memadai.

DAFTAR PUSTAKA

Abidin, M. F., Tarigan, A., & Prananingrum, L. (2023). Perancangan dan implementasi smart contract pada sistem verifikasi dokumen berbasis zero knowledge proof (ZKP) pada blockchain Polygon. Jurnal Ilmiah Informatika Komputer, 28(2), 100–111.

Dzakiy, M. I. (2020). Pemanfaatan smart contract dalam blockchain untuk mengoptimasi e-commerce. Jurnal Pemandhu.

Fajarianto, E. R., Zulfikar, P., & Mulyadi, E. (2022). Tinjauan yuridis penggunaan blockchain-smart contract dalam transaksi non-fungible token (NFT) pada PT. SAGA RIUNG INVESTAMA. Jurnal Pemandhu, 3(2), 84–97.

Ihsan, R. (2022). Peluang dan tantangan penggunaan blockchain technology pada perbankan syariah di Indonesia. E-Qien: Jurnal Ekonomi Dan Bisnis, 11(3), 1037–1049.

Irawan, B. (2023). Implementasi teknologi blockchain untuk keamanan data internet of things. Humantech Jurnal Ilmiah Multi Disiplin Indonesia, 2(9), 1944–1953.

Islami, M. J. (2017). Tantangan dalam implementasi strategi keamanan siber nasional Indonesia di tinjau dari penilaian global cybersecurity index. Jurnal Masyarakat Telematika Dan Informasi, 8(2), 137–144.

Kristianti, N., & Kurniasi, R. (2024). Peraturan dan regulasi keamanan siber di era digital. Satya Dharma: Jurnal Ilmu Hukum, 7(1), 297–310. https://ejournal.iahntp.ac.id/index.php/satya-dhamat%0APeraturan

Megawati, L., Wiharma, C., & Hasanuudin, A. (2023). Peran teknologi blockchain dalam meningkatkan keamanan dan kepastian hukum dalam transaksi kontrak di Indonesia. Jurnal Hukum Mimbar Justitia, 9(2). https://jurnal.unsur.ac.id/jmj

Olivia, B., Irine, P., Tahir, M., Ayu, N., Cholili, D. Y., Mulaikah, D., Batsul, A., & Septian, M. (2023). Implementasi kriptografi pada keamanan data menggunakan algoritma advance encryption standard (AES). Jurnal SimanteC, 11(2), 167–174.

Setianingsih, R. (2024). Analisis teknologi blockchain berperan dalam meningkatkan keamanan dan data privasi di sektor keuangan terhadap implementasi. Jurnal Ilmiah Nustantara (Jinu), 1(4), 588–596. https://doi.org/10.61722/jinu.v1i4.1841

Simanungkalit, A. (2024). Teknologi blockchain: Solusi untuk keamanan data dalam transaksi

digital. Jurnal Circle Archive, 1(6), 1–8.

Syafutra, T. R., & Suryana, E. (2022). Penerapan kriptografi modern pada pengamanan data dokumen. Jurnal Media Computer Science, 1(2), 287–294.

Vincha, C., & Satrio, J. (2024). Kemunculan ancaman siber teknologi 5G dan implikasinya terhadap ketahanan siber Indonesia. Jurnal Ketahanan Nasional, 30(2), 222–241.

Wardhana, C. S. (2024). Implementasi teknologi blockchain dalam optimalisasi keamanan database penduduk di kementerian dalam negeri. Action Research Literate, 8(4), 642–648.