



ANALISIS PERAN TEKNOLOGI BLOCKCHAIN TERHADAP KEAMANAN SIBER PADA ASET DIGITAL DI INDONESIA

Jeriko¹, Jerico Pradinata², Steven Haryanto³, Marvelius⁴, Albert Oktavianus⁵, Joosten⁶

^{1,2,3,4,5,6} Universitas Mikroskil
211120084@students.mikroskil.ac.id

Abstrak

Di Indonesia, teknologi blockchain telah menjadi cara mutakhir untuk memperkuat keamanan siber aset digital. Dengan penekanan pada keamanan informasi, integritas data, anonimitas, dan transparansi, studi ini meneliti bagaimana teknologi blockchain dapat membantu masalah keamanan digital. Melalui analisis dokumen dan studi kasus kualitatif, penelitian ini mengungkapkan bagaimana teknologi blockchain dapat melindungi aset digital dari serangan online. Temuan ini menunjukkan bagaimana desentralisasi, enkripsi, dan validasi terdesentralisasi blockchain memberikan langkah-langkah keamanan yang lebih baik. Namun, masih ada masalah dengan infrastruktur, peraturan, dan literasi teknologi yang mempengaruhi penyebarannya di Indonesia. Menurut penelitian ini, blockchain memiliki banyak harapan untuk merevolusi keamanan siber, tetapi implementasinya membutuhkan strategi yang menyeluruh.

Kata kunci: *Blockchain, Keamanan Siber, Aset Digital, Teknologi Informasi, Desentralisasi*

Abstract

In Indonesia, blockchain technology has become a cutting-edge way to strengthen the cybersecurity of digital assets. With an emphasis on information security, data integrity, anonymity, and transparency, this study examines how blockchain technology can help with digital security issues. Through document analysis and qualitative case studies, the study reveals how blockchain technology can shield digital assets from online attacks. The findings demonstrate how blockchain's decentralization, encryption, and decentralized validation provide better security measures. However, there are still issues with infrastructure, regulations, and technology literacy that affect its deployment in Indonesia. According to this study, blockchain has a lot of promise to revolutionize cybersecurity, but its implementation calls for a thorough strategy.

Keywords: *Blockchain, Cybersecurity, Digital Assets, Information Technology, Decentralization*

Article History

Received: November 2024
Reviewed: November 2024
Published: Desember 2024

Plagirism Checker No 234
Prefix DOI : Prefix DOI :
10.8734/Kohesi.v1i2.365

Copyright : Author
Publish by : Kohesi



This work is licensed under
a [Creative Commons
Attribution-NonCommercial
4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/)

1. PENDAHULUAN

Era digitalisasi telah membawa perubahan signifikan terhadap cara pengelolaan dan penyimpanan aset digital di Indonesia. Dengan pesatnya pertumbuhan adopsi teknologi digital, tantangan keamanan siber menjadi semakin kompleks dan membutuhkan solusi yang lebih canggih [1]. Dalam konteks ini, teknologi blockchain dianggap sebagai salah satu inovasi yang menjanjikan untuk meningkatkan keamanan dan integritas aset digital.

Sebagai negara dengan populasi digital yang besar, Indonesia mengalami peningkatan penggunaan aset digital yang signifikan. Menurut data Interpol *Cyber Assessment Report 2021*, pada rentang waktu Januari - September terdapat lebih dari 2,7 juta serangan siber yang terjadi



di Asia Tenggara dan Indonesia menjadi peringkat teratas dengan 1,3 juta kasus. Pada tahun 2022, terdapat 8.831 kasus kejahatan siber yang dituntut, meningkat 14x lipat dibandingkan tahun 2021 yang hanya 612 kasus yang dituntut. Selain itu, penelitian Fortinet menunjukkan bahwa serangan siber ransomware di Indonesia akan berlipat ganda pada tahun 2023 [2]. Fenomena ini menunjukkan adanya kebutuhan mendesak untuk menerapkan sistem keamanan yang lebih kuat untuk melindungi aset digital.

Teknologi *Blockchain*, dengan karakteristik desentralisasi dan kekekalan, menawarkan solusi potensial untuk mengatasi banyak kesenjangan dalam keamanan siber tradisional [3]. Sistem pencatatan terdesentralisasi yang menjadi dasar *blockchain* memungkinkan verifikasi dan validasi transaksi lebih transparan dan aman [4]. Karakteristik ini menjadikan *blockchain* sebagai teknologi yang menarik untuk digunakan dalam konteks keamanan siber, khususnya dalam perlindungan aset digital.

Meski demikian, penerapan *blockchain* dalam konteks keamanan siber di Indonesia masih menghadapi berbagai tantangan baik dari segi teknis maupun regulasi. Tujuan dari penelitian ini adalah untuk menganalisis peran teknologi *blockchain* dalam meningkatkan keamanan siber aset digital di Indonesia, dengan mempertimbangkan aspek teknis, peraturan, dan sosial ekonomi yang relevan. Kajian ini penting mengingat masih kurangnya kajian komprehensif yang menyelidiki penerapan *blockchain* untuk keamanan siber di Indonesia. Hasil penelitian tersebut diharapkan dapat memberikan kontribusi yang signifikan terhadap pengembangan kebijakan dan strategi keamanan siber nasional, khususnya terkait perlindungan aset digital.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan menerapkan metodologi studi kasus. Studi kasus dipilih untuk memberikan kajian mendalam mengenai penerapan teknologi *blockchain* untuk meningkatkan keamanan siber aset digital di Indonesia.

2.1 Desain Penelitian

Penelitian ini juga didasarkan pada desain studi kasus deskriptif yang bertujuan untuk memberikan gambaran komprehensif tentang peran teknologi *blockchain* dalam meningkatkan keamanan siber aset digital di Indonesia [5]. Pendekatan ini memungkinkan peneliti mempelajari fenomena dalam situasi dunia nyata dan mencapai pemahaman yang mendalam.

2.2 Pengumpulan Data

Data dikumpulkan melalui dua sumber utama yaitu tinjauan Pustaka yakni konten akademik terkini, termasuk artikel jurnal, konferensi, dan buku, terkait dengan *blockchain*, keamanan siber, dan tinjauan publikasi yang sistematis, dilanjutkan dengan analisis dokumen kebijakan, peraturan, dan kebijakan pemerintah dan organisasi terkait serta review laporan penelitian terkait, studi kasus, dan analisis industri. Lalu menggunakan Analisis Dokumen yang berisi kumpulan analisis dokumen peraturan, kebijakan, laporan, dan pedoman terkait implementasi *blockchain* dan keamanan siber di Indonesia. Materi ini diperoleh dari situs web pemerintah, organisasi, dan asosiasi industri terkait.

2.3 Analisis Data

Data yang terkumpul akan dianalisis menggunakan pendekatan tematik dengan mengklasifikasikan dan mengidentifikasi tema-tema utama dari tinjauan literatur dan analisis dokumen, lalu dilanjutkan dengan analisis silang dan sintesis data dari berbagai sumber untuk mendapatkan pemahaman komprehensif [6]. Terakhir dengan melakukan penafsiran hasil penelitian dan menarik kesimpulan.

Analisis data dilakukan dengan menggunakan perangkat lunak pengolah data kualitatif seperti NVivo dan Atlas.ti untuk memfasilitasi pengkodean, klasifikasi, dan visualisasi data [7][8].

2.4 Validitas dan Reliabilitas



Beberapa langkah dilakukan untuk menjamin validitas dan reliabilitas hasil penelitian seperti Triangulasi data-data berbeda untuk memverifikasi dan memperkaya hasil, *Audit Trail* yaitu mendokumentasikan secara merinci proses pengumpulan, analisis, dan interpretasi data sehingga dapat diaudit [9] dan terakhir *Peer Check* yaitu Melibatkan rekan peneliti dalam tinjauan kritis terhadap proses dan temuan penelitian.

Kerangka penelitian ini diharapkan dapat memberikan analisis yang komprehensif dan andal mengenai peran teknologi *blockchain* dalam meningkatkan keamanan siber aset digital di Indonesia.

3. HASIL DAN PEMBAHASAN

3.1 Penerapan Teknologi *Blockchain* untuk Keamanan terhadap keamanan siber pada aset

Blockchain adalah teknologi buku besar digital yang revolusioner yang pertama kali dikenal luas melalui cryptocurrency Bitcoin. Pada intinya, ia berfungsi sebagai sistem terdesentralisasi yang menyimpan transaksi sebagai blok yang saling terhubung, diamankan melalui metode hashing kriptografi [10]. Sistem ini bekerja dengan cara menyimpan data dalam blok-blok yang saling terhubung, menciptakan rantai data yang sulit dimanipulasi. Lima aspek utama keamanan yang ditawarkan blockchain meliputi: keamanan informasi melalui sistem penyimpanan data yang tidak bisa diedit, integritas data yang dijamin melalui validasi transaksi oleh seluruh node dalam jaringan, anonimitas pengguna melalui penggunaan alamat digital, transparansi data yang memungkinkan akses terbuka namun aman, serta keandalan sistem melalui penyimpanan data yang tersebar di berbagai node [11]. Keamanan data sebagai aset digital telah menjadi prioritas utama di era digitalisasi, mengingat perannya yang sangat krusial dalam pengambilan keputusan bisnis dan operasional organisasi [12].

Keandalan blockchain tercermin dari arsitektur jaringan terdesentralisasinya, yang memungkinkan data tetap dapat diakses meskipun terjadi kerusakan pada salah satu node. Karakteristik ini membuat blockchain tidak hanya sekadar teknologi penyimpanan data, melainkan sistem yang tangguh, aman, dan dapat diandalkan untuk berbagai keperluan di era digital. Dengan demikian, blockchain memiliki potensi besar untuk mentransformasi berbagai bidang, mulai dari keuangan, manajemen rantai pasok, hingga sistem pencatatan digital yang memerlukan keamanan dan integritas tinggi [13].

Amerika Serikat, yang awalnya mengklasifikasikan cryptocurrency sebagai komoditas, kini mulai mengkategorikannya sebagai alat pembayaran sah. Dinamika ini menunjukkan urgensi dalam merumuskan regulasi yang adaptif terhadap inovasi teknologi keuangan [14]. Bitcoin, sebagai salah satu pionir mata uang digital, dibangun di atas fondasi teknologi blockchain. Keamanan dan integritas transaksi yang dijamin oleh teknologi ini menjadi katalis utama dalam percepatan adopsi mata uang digital secara global [15]. Keamanan transaksi menjadi salah satu keamanan fitur dalam blockchain, dengan sistem pencatatan yang tidak dapat dimanipulasi dan transparansi yang terjamin dalam setiap transaksi [16]. Di Indonesia, blockchain semakin dilirik sebagai solusi dalam menjaga integritas data di berbagai sektor, seperti keuangan, e-commerce, dan sektor pemerintahan.

- **Keamanan Informasi dan Integritas Data:** Dalam sistem *blockchain*, setiap transaksi dicatat dalam blok yang terhubung dan diverifikasi oleh seluruh jaringan, menciptakan keamanan yang lebih baik karena data tidak dapat diubah tanpa persetujuan mayoritas. Menurut jurnal dari Isma Elan Maulani, Tedi Herdianto, Dwi Febri Syawaludin, dan Medika Oga Laksana (2023), teknologi ini dapat mengurangi risiko peretasan pada data digital, terutama dalam sektor keuangan yang sering menjadi target serangan siber [11].
- **Anonimitas dan Privasi Pengguna:** *Blockchain* memungkinkan anonimitas pengguna dengan mengandalkan alamat digital alih-alih identitas asli pengguna. Fitur ini menjaga privasi data pengguna dan mempersulit penjahat siber untuk melacak transaksi secara langsung. Penelitian oleh Riskha Setianingsih dan Muhammad Irwan Padli Nasution (2024) menunjukkan bahwa *blockchain* dapat meningkatkan perlindungan privasi dalam transaksi



digital, yang sangat penting di era digital saat ini, di mana pelanggaran privasi sering kali terjadi [17].

- **Transparansi dan Auditabilitas:** *Blockchain* memungkinkan transparansi yang tinggi dalam setiap transaksi, sehingga semua pihak dapat melihat riwayat transaksi yang telah terjadi tanpa bisa memodifikasi data yang sudah ada. Penelitian dari Tito Wira Eka Suryawijaya (2023) menunjukkan bahwa fitur transparansi ini menjadikan *blockchain* sebagai pilihan ideal untuk menghindari penipuan dan memastikan akuntabilitas [12].

3.2 Tantangan Implementasi *Blockchain* di Indonesia

Era transformasi digital di Indonesia menunjukkan potensi signifikan penggunaan teknologi *blockchain* dalam meningkatkan keamanan dan efisiensi sistem digital lintas berbagai sektor. Pemerintah Indonesia telah menginisiasi beberapa proyek strategis yang memanfaatkan teknologi *blockchain*, termasuk verifikasi sertifikat pendidikan, manajemen data medis, dan sistem pembayaran digital. Dalam konteks pendidikan, *blockchain* memungkinkan proses verifikasi sertifikat yang cepat, akurat, dan transparan, secara substansial mengurangi risiko pemalsuan dokumen dan memfasilitasi proses rekrutmen yang lebih andal [18]. Meskipun *blockchain* memiliki banyak manfaat dalam meningkatkan keamanan siber, penerapannya di Indonesia masih menghadapi berbagai kendala, antara lain:

- **Keterbatasan Infrastruktur Teknologi dan Sumber Daya Manusia:** Penerapan *blockchain* memerlukan dukungan infrastruktur yang kuat dan tenaga ahli yang menguasai teknologi ini. Di Indonesia, adopsi teknologi baru sering terkendala oleh terbatasnya infrastruktur digital di beberapa wilayah. Menurut Kurniawan (2019), Indonesia masih memerlukan investasi besar dalam pengembangan infrastruktur dan pelatihan tenaga ahli untuk mendukung implementasi *blockchain* secara merata [19].
- **Regulasi yang Belum Matang:** Peraturan yang mengatur penggunaan *blockchain* di Indonesia masih dalam tahap perkembangan, khususnya dalam konteks keamanan siber. Regulasi yang jelas dan mendukung sangat penting untuk memberikan kepastian hukum bagi pengguna dan pengembang *blockchain*. Leny Megawati, Cecep Wiharna, Asep Hasanudin (2023) menekankan pentingnya regulasi yang adaptif untuk mengikuti perkembangan teknologi *blockchain*, agar inovasi ini dapat dimanfaatkan secara maksimal [20].
- **Kesadaran dan Pemahaman Publik yang Rendah:** Masih banyak pihak di Indonesia yang belum memahami manfaat *blockchain*, baik di sektor publik maupun swasta. Penelitian oleh Violeta Michiko Kawengian, Marthen Y. Tampanguma, Grace H. Tampongangoy (2024) mengindikasikan bahwa rendahnya literasi akan teknologi ini menjadi hambatan dalam adopsi teknologi *blockchain* [21].

3.3 Transparansi terhadap Keamanan dan Transaksi Aset

Teknologi *blockchain* secara luas sudah diterima sebagai teknologi yang memiliki keunggulan untuk dapat melakukan traceability dan transparency dalam kegiatan bisnis. Teknologi *blockchain* juga dikenal dengan sebutan Distributed Ledger Technology (DLT) yang merupakan sistem pencatatan terdistribusi dan terdesentralisasi untuk memberikan transparansi, keamanan data, dan juga integritas (Subramanian et al., 2020) [22]. Teknologi Distributed Ledger (DLT) menghadirkan transformasi fundamental dalam transparansi transaksi aset digital, dengan potensi inovasi yang belum pernah terjadi sejak kemunculan internet. Keunggulan DLT terletak pada kemampuannya mengamankan transaksi melalui mekanisme desentralisasi yang membuat setiap transaksi tercatat secara permanen, tidak dapat dimanipulasi, dan dapat diverifikasi oleh seluruh jaringan [23]. Sebagai jenis khusus teknologi buku besar terdistribusi (DLT), *blockchain* menyimpan data terenkripsi di seluruh jaringan peer-to-peer, menghubungkan "blok" informasi yang berdekatan ke dalam "rantai." Informasi yang tersedia untuk semua peserta jaringan adalah semua transaksi informasi di *blockchain* [24].

Keunggulan *Hyperledger Fabric* kerangka *blockchain* berpermisi yang menawarkan solusi transparansi dan keamanan aset digital melalui mekanisme kontrol akses ketat, konsensus fleksibel, dan chaincode yang dapat dikustomisasi. Platform ini memungkinkan organisasi



membangun jaringan blockchain aman dan terpercaya, di mana hanya node tepercaya yang dapat berpartisipasi, sehingga menjamin integritas dan kerahasiaan transaksi aset dalam berbagai industri seperti keuangan, rantai pasok, dan kesehatan [25]. Fabric adalah blockchain yang diizinkan, yang berarti hanya entitas yang berwenang yang dapat menjadi bagian dari jaringan. Arsitektur yang diizinkan memungkinkan bisnis untuk tetap bersifat pribadi, rahasia, dan memiliki skalabilitas yang kuat [26]. Pemanfaatan blockchain *hyperledger fabric* dalam sistem informasi berhasil meningkatkan transparansi alur peminjaman dengan menciptakan catatan transaksi yang tidak dapat diubah dan dapat dilacak oleh semua partisipan [27]. Hyperledger Fabric terdiri dari 4 aspek berikut: Pertama, kriptografi yang tidak merata dan bukti tanpa informasi memisahkan informasi transaksi dari catatan on-chain, privasi yang protektif dari algoritma yang mendasarinya. Kedua, penyedia kontrol sertifikat virtual memastikan legitimasi organisasi di blockchain. Ketiga, tata letak multi-saluran memisahkan statistik di antara saluran yang unik. Terakhir, rangkaian informasi privasi juga memenuhi kebutuhan untuk mengisolasi informasi privasi di antara lembaga-lembaga unik di saluran yang sama [28].

Keunggulan *Smart contract* merupakan inovasi revolusioner dalam teknologi blockchain yang menghadirkan sistem transaksi dan keamanan aset yang terdesentralisasi, aman, dan transparan. Melalui otomatisasi eksekusi kontrak tanpa perantara, smart contract memungkinkan interaksi digital yang andal dengan menjamin integritas data melalui blockchain yang tidak dapat diubah. Keunggulannya terletak pada kemampuan mengurangi risiko kesalahan dan penipuan, meningkatkan efisiensi transaksi, serta memberikan mekanisme kontrol yang transparan dan terpercaya bagi para pihak yang terlibat dalam perjanjian digital [29]. Peredaran produk palsu dapat ditekan secara signifikan melalui penerapan *smart contract*. Teknologi *blockchain* yang mendasari *smart contract* menyediakan platform yang aman dan transparan, sehingga mampu memastikan keaslian dan keamanan produk. Dengan demikian, kepercayaan konsumen terhadap produk yang dibeli dapat ditingkatkan secara signifikan [30].

4. KESIMPULAN

Relevansi penting dari teknologi blockchain dalam meningkatkan keamanan siber aset digital di Indonesia ditunjukkan oleh penelitian ini. Proses desentralisasi Blockchain yang unik menawarkan banyak manfaat, termasuk kemampuan untuk memastikan integritas data, menciptakan sistem pencatatan yang tidak dapat diubah, dan memberikan transparansi transaksi yang aman. Keamanan informasi yang tidak dapat diedit, validasi data yang terdesentralisasi, anonimitas pengguna, transparansi yang terkendali, dan stabilitas sistem melalui berbagai distribusi data merupakan lima pilar keamanan utama yang ditawarkan oleh teknologi ini. Adopsi Blockchain di Indonesia saat ini menghadapi banyak kendala, seperti infrastruktur teknologi yang tidak memadai, peraturan yang tidak jelas, dan tingkat literasi digital yang rendah, terlepas dari potensinya yang revolusioner. Pendekatan sistematis yang mencakup investasi berkelanjutan dalam infrastruktur digital, pelatihan sumber daya manusia, dan pembuatan kerangka kerja peraturan yang dapat beradaptasi diperlukan untuk memaksimalkan potensinya. Untuk mencapai transformasi keamanan siber yang menyeluruh di Indonesia, penelitian ini menyimpulkan bahwa blockchain lebih dari sekadar teknologi; blockchain merupakan paradigma baru dalam keamanan digital yang membutuhkan kerja sama lintas sektoral antara pemerintah, bisnis, dan akademisi.

Daftar Pustaka

- [1] E. Susanto, Lady Antira, K. Kevin, E. Stanzah, and A. A. Majid, "MANAJEMEN KEAMANAN CYBER DI ERA DIGITAL," *Journal of Business And Entrepreneurship*, vol. 11, no. 1, p. 23, Jun. 2023, doi: 10.46273/job.e.v11i1.365.
- [2] F. Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia," *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum*, vol. 2, no. 1, pp. 8–16, Jan. 2024, doi: 10.32520/albahts.v2i1.3044.



- [3] Baihaqsani, A. Kusyanti, and P. H. Trisnawan, "Implementasi Teknologi Blockchain dengan Sistem Smart Contract pada Klaim Asuransi," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 11, no. 5, pp. 1105–1112, Oct. 2024, doi: 10.25126/jtiik.1078016.
- [4] L. L. Pratiwi, "Implementasi Blockchain Pada Akuntansi dan Audit di Indonesia," *Fair Value: Jurnal Ilmiah Akuntansi dan Keuangan*, vol. 4, no. 6, pp. 2185–2203, Jan. 2022, doi: 10.32670/fairvalue.v5i01.873.
- [5] E. Jarva *et al.*, "Healthcare professionals' perceptions of digital health competence: A qualitative descriptive study," *Nurs Open*, vol. 9, no. 2, pp. 1379–1393, Mar. 2022, doi: 10.1002/nop2.1184.
- [6] C. Wendelborn, M. Anger, and C. Schickhardt, "What is data stewardship? Towards a comprehensive understanding," *J Biomed Inform*, vol. 140, p. 104337, Apr. 2023, doi: 10.1016/j.jbi.2023.104337.
- [7] D. B. Allsop, J. M. Chelladurai, E. R. Kimball, L. D. Marks, and J. J. Hendricks, "Qualitative Methods with Nvivo Software: A Practical Guide for Analyzing Qualitative Data," *Psych*, vol. 4, no. 2, pp. 142–159, Mar. 2022, doi: 10.3390/psych4020013.
- [8] Y. Choe, J. Lee, and G. Lee, "Exploring Values via the Innovative Application of Social Media with Parks Amid COVID-19: A Qualitative Content Analysis of Text and Images Using ATLAS.ti," *Sustainability*, vol. 14, no. 20, p. 13026, Oct. 2022, doi: 10.3390/su142013026.
- [9] M. Ngoepe and L. Kenosi, "Confronting Jenkinson's canon: reimagining the 'destruction and selection of modern archives' through the Auditor-General of South Africa's financial audit trail," *Archives and Records*, vol. 43, no. 2, pp. 166–176, May 2022, doi: 10.1080/23257962.2022.2048639.
- [10] T. Huynh-The *et al.*, "Blockchain for the metaverse: A Review," *Future Generation Computer Systems*, vol. 143, pp. 401–419, Jun. 2023, doi: 10.1016/j.future.2023.02.008.
- [11] I. Elan Maulani, T. Herdianto, D. Febri Syawaludin, and M. Oga Laksana, "Penerapan Teknologi Blockchain Pada Sistem Keamanan Informasi," *Jurnal Sosial Teknologi*, vol. 3, no. 2, pp. 99–102, Feb. 2023, doi: 10.59188/jurnalsostech.v3i2.634.
- [12] T. W. E. Suryawijaya, "Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia," *Jurnal Studi Kebijakan Publik*, vol. 2, no. 1, pp. 55–68, May 2023, doi: 10.21787/jskp.2.2023.55-68.
- [13] I. Elan Maulani, T. Herdianto, D. Febri Syawaludin, and M. Oga Laksana, "Penerapan Teknologi Blockchain Pada Sistem Keamanan Informasi," *Jurnal Sosial Teknologi*, vol. 3, no. 2, pp. 99–102, Feb. 2023, doi: 10.36418/jurnalsostech.v3i2.634.
- [14] Y. Sobikhoh Nawaidah, D. Sadia Wati, P. Kinanti, R. Mahesa, F. Hariz, and P. Suryaning Ramadhani, "Melintasi Era Digital Dengan Menganalisis Hukum Cryptocurrency dan Blockchain Dalam Yurisprudensi Modern," 2023, [Online]. Available: <https://j-innovative.org/index.php/Innovative>
- [15] M. S. Abstrak, "Revolusi Teknologi Blockchain: Dampaknya pada Keamanan dan Integritas Data."
- [16] E. S. Wicaksono, J. M. Keuangan, M. Manajemen, I. Artikel, and S. Artikel, "Bridging: Journal of Islamic Digital Economic and Management KEJATUHAN FTX DAN PELAJARAN PENTING BAGI SOLUSI CRYPTO CUSTODY: ANALISIS RISIKO SISTEMIK DAN PERLINDUNGAN ASET," vol. 1, no. 1, 2023, [Online]. Available: <https://journal.alshobar.or.id/index.php/bridging>
- [17] R. Setianingsih, U. I. Negeri, and S. Utara, "Analisis Teknologi Blockchain Berperan dalam Meningkatkan Keamanan dan Data Privasi di Sektor Keuangan Terhadap Implementasi," *Jurnal Ilmiah Nusantara (JINU)*, vol. 1, no. 4, pp. 3047–9673, 2024, doi: 10.61722/jinu.v1i4.1841.
- [18] T. W. E. Suryawijaya, "Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia," *Jurnal Studi Kebijakan Publik*, vol. 2, no. 1, pp. 55–68, May 2023, doi: 10.21787/jskp.2.2023.55-68.



- [19] Lisdawati, P. P. Saputra, E. Yulianto, H. Lase, and Daryanto, "Implementasi Teknologi Blockchain Dalam Akuntansi Keuangan: Peluang Dan Tantangan Bagi Perusahaan Di Indonesia," 2024.
- [20] L. Megawati, C. Wiharma, and A. Hasanudin, "PERAN TEKNOLOGI BLOCKCHAIN DALAM MENINGKATKAN KEAMANAN DAN KEPASTIAN HUKUM DALAM TRANSAKSI KONTRAK DI INDONESIA," Online, 2023. [Online]. Available: <https://jurnal.unsur.ac.id/jmj>
- [21] V. M. Kawengian, M. Y. Tampamguma, and G. H. Tampongangoy, "TINJAUAN HUKUM PERAN BANK SENTRAL TERHADAP PENGGUNAAN TEKNOLOGI BLOCKCHAIN DALAM TRANSAKSI KEUANGAN DI INDONESIA 1 Oleh," 2024. [Online]. Available: <https://klc2.kemenkeu.go.id/document/2021/10/>
- [22] T. D. Maharani, A. Sarjito, and C. S. Marnani, "PENERAPAN TEKNOLOGI BLOCKCHAIN DALAM MANAJEMEN LOGISTIK PERTAHANAN," *JAMI: Jurnal Ahli Muda Indonesia*, vol. 4, no. 2, pp. 136–147, Dec. 2023, doi: 10.46510/jami.v4i2.155.
- [23] K. R. Ballamudi, "Blockchain as a Type of Distributed Ledger Technology," *Asian Journal of Humanity, Art and Literature*, vol. 3, no. 2, pp. 127–136, Dec. 2016, doi: 10.18034/ajhal.v3i2.528.
- [24] M. Hasnain, F. R. Albogamy, S. S. Alamri, I. Ghani, and B. Mehboob, "The Hyperledger fabric as a Blockchain framework preserves the security of electronic health records," *Front Public Health*, vol. 11, Nov. 2023, doi: 10.3389/fpubh.2023.1272787.
- [25] S. K. Jena, B. Kumar, B. Mohanty, A. Singhal, and R. C. Barik, "An advanced blockchain-based hyperledger fabric solution for tracing fraudulent claims in the healthcare industry," *Decision Analytics Journal*, vol. 10, p. 100411, Mar. 2024, doi: 10.1016/j.dajour.2024.100411.
- [26] Y. Ucbas, A. Eleyan, M. Hammoudeh, and M. Alohal, "Performance and Scalability Analysis of Ethereum and Hyperledger Fabric," *IEEE Access*, vol. 11, pp. 67156–67167, 2023, doi: 10.1109/ACCESS.2023.3291618.
- [27] F. Gani Setyawan and H. Kabetta, "Kajian Implementasi Blockchain dalam Sistem Manajemen Aset pada Gudang Logistik Instansi XYZ," 2024.
- [28] K. Kumutha, S. Jayalakshmi, and P. SriPriya, "Data security mechanism of hyperledger fabric and its application in academic documents verification system," *Int J Health Sci (Qassim)*, pp. 4394–4403, Apr. 2022, doi: 10.53730/ijhs.v6nS3.6821.
- [29] Andini Eka Budiyo, "ANALISIS YURIDIS PENGGUNAAN SMART CONTRACT DALAM PERSPEKTIF ASAS KEBEBASAN BERKONTRAK," *JOURNAL SAINS STUDENT RESEARCH*, vol. 1, no. 1, pp. 815–827, Oct. 2023, doi: 10.61722/jssr.v1i1.402.
- [30] A. Hermawan, D. P. S. Karlim, J. Junaedi, and B. Daniawan, "Pemanfaatan Smart Contract dalam Transformasi Supply Chain melalui Teknologi Blockchain," *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, vol. 9, no. 3, p. 471, Dec. 2023, doi: 10.26418/jp.v9i3.69328.