



PEMANFAATAN BLOCKCHAIN DALAM PENCEGAHAN CYBERCRIME PADA TRANSAKSI DIGITAL

Nazwa Azzahra¹, Agis Aulia², Alif Firmansyah³, Asmak UI Hosnah⁴

^{1,2,3,4}Faculty of Law, Pakuan University, Indonesia

Email : nazwaazzahra16@gmail.com¹, auliaagis5@gmail.com², alifrmnsyh23@gmail.com³,
asmak.hosnah@unpak.ac.id⁴

Received 23-08-2025 | Revised form 25-09-2025 | Accepted 01-11-2025

Abstract

The very rapid development of information technology has encouraged digital transformation in various sectors, especially in electronic financial transaction systems. However, this progress is also accompanied by increasing threats of cybercrime such as hacking, data theft and manipulation of digital transactions. This research aims to analyze the use of blockchain technology as a preventive solution to cybercrime in digital transactions. Blockchain has great potential in increasing the transparency, integrity and security of transaction data through decentralized mechanisms and cryptographic verification that are difficult to manipulate. With an immutable recording system called an immutable ledger, blockchain is able to prevent fraud, data tampering and illegal access. However, its implementation still faces challenges in the form of regulatory limitations, infrastructure costs and also the need for adequate digital literacy. In conclusion, the use of blockchain is a strategic and innovative step in strengthening the cyber security system and building public trust in digital transactions in the digital economy era.

Keywords : blockchain, digital transactions, cyber security

Abstrak

Perkembangan teknologi informasi yang sangat pesat telah mendorong transformasi digital dalam berbagai sektor terutama pada sistem transaksi keuangan elektronik. Namun, kemajuan ini juga diiringi dengan meningkatnya ancaman kejahatan siber atau cybercrime seperti peretasan, pencurian data dan manipulasi transaksi digital. Penelitian ini bertujuan untuk menganalisis pemanfaatan teknologi *blockchain* sebagai solusi preventif terhadap tindak kejahatan siber dalam transaksi digital. *Blockchain* memiliki potensi besar dalam meningkatkan transparansi, integritas, dan keamanan data transaksi melalui mekanisme desentralisasi dan verifikasi kriptografi yang sulit dimanipulasi. Dengan sistem pencatatan yang tidak dapat diubah yang disebut dengan *immutable ledger*, *blockchain* mampu mencegah terjadinya penipuan, *data tampering* dan juga tindakan akses ilegal. Namun demikian, implementasinya masih menghadapi tantangan berupa keterbatasan regulasi, biaya infrastruktur dan juga kebutuhan akan literasi digital yang memadai. Kesimpulannya, pemanfaatan *blockchain* merupakan langkah strategis dan inovatif dalam memperkuat sistem keamanan siber dan membangun kepercayaan publik terhadap transaksi digital di era ekonomi digital.

Kata Kunci : blockchain, transaksi digital, keamanan siber

This is an open access article under the CC BY-NC-SA license.



A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan yang signifikan dalam sistem transaksi ekonomi global. Digitalisasi transaksi keuangan

melalui *e-commerce*, *mobile banking* dan juga *digital payment* lainnya menjadi bentuk nyata dari kemajuan teknologi yang menawarkan kemudahan, efisiensi dan aksesibilitas yang tinggi bagi masyarakat luas. Namun, darinya kemajuan tersebut juga menimbulkan berbagai tantangan baru dalam aspek keamanan siber atau dalam Bahasa Inggrisnya *cybersecurity*, terutama terkait meningkatnya kasus *cybercrime* seperti contohnya seperti *phishing*, *data breach*, *identity theft* serta manipulasi transaksi digital. Menurut laporan dari berbagai lembaga keamanan digital, kerugian akibat kejahatan siber terus meningkat setiap tahunnya, hal ini menunjukkan lemahnya sistem keamanan konvensional yang masih bergantung pada otoritas terpusat. Dalam konteks inilah teknologi *blockchain* hadir sebagai alternatif solusi yang menawarkan pendekatan baru dalam menjamin keamanan, transparansi dan juga integritas data. *Blockchain* merupakan sistem pencatatan digital yang bersifat terdesentralisasi dan didistribusikan pada jaringan komputer, sehingga setiap transaksi terekam dalam blok-blok yang saling terhubung secara kriptografis. Basis data *blockchain* menyimpan data dalam blok yang dihubungkan bersama dalam sebuah rantai¹. Karakteristik ini membuat *blockchain* menjadi sistem yang hampir mustahil untuk dimanipulasi dikarenakan setiap perubahan harus mendapat persetujuan mayoritas jaringan. Dengan demikian, teknologi ini mampu menciptakan sistem yang lebih aman dari ancaman manipulasi dan penipuan data, serta dapat digunakan sebagai instrumen pencegahan terhadap tindak *cybercrime*.

Pemanfaatan *blockchain* juga memiliki dimensi hukum dan sosial yang penting. Dalam transaksi digital, kepercayaan menjadi faktor utama yang menentukan keberlangsungan sistem ekonomi digital. *Blockchain* sebagai sistem pencatatan digital mampu membangun kepercayaan tersebut melalui mekanisme transparansi dan akuntabilitas otomatis, tanpa bergantung pada pihak ketiga. Namun, di Indonesia sendiri, penerapan *blockchain* masih menghadapi sejumlah kendala, baik dari sisi regulasi, kesiapan infrastruktur maupun literasi digital masyarakat. Hal ini menimbulkan pertanyaan mengenai sejauh mana *blockchain* dapat diimplementasikan secara efektif dalam mencegah kejahatan siber di sektor transaksi digital. Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis potensi dan tantangan pemanfaatan *blockchain* dalam pencegahan *cybercrime* pada transaksi digital. Penelitian ini diharapkan dapat memberikan kontribusi teoretis dan praktis dalam pengembangan sistem keamanan siber yang lebih kuat, serta menjadi dasar bagi pembuat kebijakan dalam merumuskan regulasi yang mendukung penerapan teknologi *blockchain* di Indonesia.

¹ Aws.amazon. "Apa itu Teknologi Blockchain" <https://aws.amazon.com/id/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc> diakses 26 Oktober 2025

B. METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi kepustakaan (*library research*). Metode ini dipilih karena fokus penelitian terletak pada analisis konseptual dan normatif terhadap pemanfaatan teknologi *blockchain* sebagai instrumen pencegahan kejahatan siber dalam transaksi digital, bukan pada pengujian empiris di lapangan. Melalui pendekatan ini, peneliti berusaha menggambarkan secara sistematis, faktual, dan akurat mengenai karakteristik, fungsi, serta potensi penerapan *blockchain* dalam memperkuat sistem keamanan siber. Jenis penelitian ini bersifat kualitatif, dengan pendekatan normatif-yuridis dan teknologis. Pendekatan normatif-yuridis digunakan untuk menganalisis aspek hukum yang berkaitan dengan perlindungan data dan transaksi elektronik berdasarkan peraturan perundang-undangan di Indonesia, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta peraturan turunannya. Data yang digunakan dalam penelitian ini terdiri dari data primer, yaitu bahan hukum utama seperti undang-undang, peraturan pemerintah, dan kebijakan terkait transaksi digital dan keamanan siber. Selain itu juga, penggunaan data sekunder digunakan didalam penelitian ini meliputi literatur akademik, jurnal ilmiah, hasil penelitian terdahulu, laporan lembaga keamanan siber, artikel ilmiah, dan publikasi teknologi yang relevan dengan topik penelitian. Seluruh data diperoleh melalui penelusuran sumber-sumber ilmiah kredibel dalam bentuk daring.

C. ANALISA DAN PEMBAHASAN

Blockchain merupakan inovasi teknologi yang bekerja dengan prinsip desentralisasi yang di mana setiap data atau transaksi tidak disimpan pada satu server pusat, tetapi tersebar ke berbagai node dalam jaringan. Node Jaringan merupakan perangkat titik aktif didalam suatu jaringan yang mampu membuat, mengirim data ataupun bahkan memproses data. Diambil dari bahasa latin, yakni *nodus* (simpul), pengertian node adalah bagian dari jaringan fisik dalam sistem komputer yang berfungsi sebagai saluran komunikasi karena menghubungkan satu perangkat ke perangkat lainnya dalam pendistribusian data atau informasi². Setiap blok data saling terhubung secara kriptografis, membentuk rantai yang tidak dapat diubah tanpa persetujuan mayoritas node dalam sistem. Karakteristik ini menjadikan *blockchain* memiliki tingkat keamanan yang tinggi karena sulit diretas atau dimanipulasi.

Dalam konteks transaksi digital, *blockchain* menghadirkan tiga nilai utama, yaitu transparansi, integritas data, dan immutability atau ketidakmampuan untuk diubah. Transparansi memastikan bahwa semua pihak yang berpartisipasi dapat memverifikasi

² Jagoan Hosting Team, "Node Adalah: Pengertian dan Fungsinya pada Jaringan Komputer" <https://www.jagoanhosting.com/blog/node-adalah/> diakses 26 Oktober 2025

transaksi tanpa mengorbankan kerahasiaan data pribadi, sementara integritas data menjamin keaslian dan keutuhan catatan digital. Sifat *immutable ledger* menjadikan *blockchain* sebagai instrumen efektif untuk mencegah terjadinya *data tampering*, manipulasi transaksi, dan pemalsuan identitas yang sering terjadi dalam *cybercrime*.

1. Karakteristik Teknologi Blockchain sebagai Fondasi Keamanan Digital

Teknologi *blockchain* lahir dari kebutuhan untuk menciptakan sistem pencatatan digital yang aman, transparan dan juga bebas dari manipulasi oleh pihak-pihak tertentu. Dalam peran teknisnya, *blockchain* merupakan buku besar digital atau *distributed ledger* yang didalamnya terdiri atas blok-blok data yang saling terhubung melalui algoritma kriptografi. Setiap blok menyimpan informasi transaksi yang diverifikasi oleh jaringan komputer independen yang disebut sebagai *nodes* sehingga setiap perubahan atau pemalsuan data hampir tidak mungkin dilakukan tanpa sepengetahuan seluruh jaringan. Ciri utama yang membedakan *blockchain* dari sistem konvensional adalah sifatnya yang terdesentralisasi, *immutable* dan transparan. Arti dari Desentralisasi didalam *blockchain* berarti didalamnya tidak ada otoritas tunggal yang mengendalikan data sehingga hal ini mengurangi risiko kebocoran akibat peretasan server pusat. *Immutability* didalam *blockchain* memastikan bahwa setiap transaksi yang telah dicatat tidak dapat dihapus ataupun diubah, sehingga meningkatkan integritas data. Dan yang terakhir yaitu Transparansi memungkinkan seluruh partisipan jaringan untuk memverifikasi transaksi tanpa harus mengandalkan pihak ketiga.

Kombinasi dari ketiga elemen tersebut menjadikan *blockchain* sebagai teknologi dengan tingkat keamanan tinggi, terutama dalam konteks transaksi digital yang rentan terhadap serangan *cybercrime*. Teknologi ini juga menyediakan tingkat keamanan yang tinggi melalui penggunaan enkripsi yang kuat dan mekanisme konsensus yang memastikan integritas data³. Dalam dunia perbankan dan keuangan digital, sistem ini dapat menjadi dasar bagi mekanisme pertukaran data dan nilai yang terpercaya serta tahan terhadap manipulasi.

2. Relevansi Blockchain terhadap Pencegahan Cybercrime dalam Transaksi Digital

Perkembangan ekonomi digital membawa kemudahan sekaligus risiko baru. Meningkatnya jumlah transaksi elektronik memicu lonjakan kasus kejahatan siber seperti *phishing*, *ransomware*, *identity theft* dan juga *data breach*. Modus operandi pelaku kejahatan semakin kompleks yang bermula dari pemalsuan data digital, penggunaan *malware* hingga manipulasi sistem keuangan berbasis internet. Sistem

³ Siahaan, P. Y., & Ng, J. (2024). Analisis implementasi teknologi blockchain dalam meningkatkan transparansi dan kepercayaan di sektor keuangan di Indonesia. *J. Sist. Inf. dan Ilmu Komput*, 2(4). Hlm. 09-31

keamanan konvensional yang berlandaskan otoritas terpusat sering kali menjadi sasaran empuk, karena satu celah keamanan dapat mengakibatkan kebocoran data secara masif. Di sinilah *blockchain* menawarkan paradigma baru: keamanan melalui konsensus kolektif dan verifikasi kriptografis. Setiap transaksi dalam jaringan *blockchain* harus disetujui oleh mayoritas node melalui mekanisme seperti *Proof of Work* atau yang disingkat POW atau *Proof of Stake* atau yang disingkat POS. Hal ini menjadikan pemalsuan data hampir mustahil dilakukan, karena untuk mengubah satu blok saja, pelaku harus menguasai lebih dari 50% node jaringan secara bersamaan, yang secara teknis dan finansial sangat sulit dilakukan. Selain itu, keberadaan *smart contract* program otomatis yang tereksekusi sesuai dengan kondisi yang telah ditetapkan memperkecil peluang manipulasi manusia. Dalam konteks transaksi digital, *smart contract* memastikan perjanjian berjalan otomatis tanpa intervensi pihak ketiga. Misalnya, dalam transaksi jual-beli online, sistem dapat mengatur agar dana baru diteruskan kepada penjual setelah pembeli mengonfirmasi penerimaan barang. Ini meminimalisasi risiko penipuan dan kecurangan. Dengan demikian, *blockchain* tidak hanya berperan sebagai media penyimpanan data yang aman, tetapi juga sebagai sistem pengawasan terdistribusi yang efektif dalam mencegah tindak kejahatan siber.

2. Peluang dan Strategi Penguatan Keamanan Siber Melalui Blockchain

Untuk memaksimalkan potensi *blockchain* dalam pencegahan *cybercrime*, diperlukan strategi kolaboratif yang melibatkan semua pemangku kepentingan. Mulai dari pemerintahan yang harus menyusun regulasi yang bersifat *adaptive regulation*, yang tidak hanya bersifat represif tetapi juga inovatif, dengan membuka ruang untuk *sandbox policy* yaitu suatu mekanisme uji coba penerapan *blockchain* dalam sistem keuangan dan administrasi publik. Rasa aman dan tenteram yang dimaksud Adalah keadaan tenteram, tenang tanpa rasa khawatir akan adanya ancaman atau tindakan yang akan menimbulkan kerugian bagi seseorang atau masyarakat⁴. Selain itu, dari sisi industri teknologi dan lembaga keuangan, diperlukannya pengintegrasian *blockchain* dalam sistem audit dan verifikasi transaksi guna meningkatkan keamanan internal.

Lembaga pendidikan dan juga riset memiliki peran dalam meningkatkan literasi dan riset terapan mengenai keamanan siber dan kriptografi. Serta Masyarakat digital perlu didorong untuk memahami pentingnya keamanan data pribadi serta menggunakan platform yang memanfaatkan *blockchain* untuk transaksi yang lebih aman.

⁴ Hutabarat, S. A., Karina, I., Banjarnahor, J. W., ul Hosnah, A., & Asmarani, N. (2024). *Pengantar Hukum Pidana: Teori dan Implementasi pada Era Revolusi Industri 4.0 menuju Era Society 5.0*. PT. Sonpedia Publishing Indonesia. hlm. 4-5

Implementasi *blockchain* dalam transaksi digital juga dapat mendukung visi pemerintah menuju Transformasi Digital Nasional 2045, dengan menciptakan ekosistem ekonomi digital yang tangguh, transparan dan juga berkeadilan. Dalam jangka panjang, *blockchain* dapat menjadi pondasi bagi sistem administrasi publik, perpajakan, hingga tata kelola hukum yang lebih efisien dan bebas manipulasi.

D. KESIMPULAN

Berdasarkan hasil analisis terhadap karakteristik teknologi *blockchain*, relevansinya dalam pencegahan *cybercrime*, serta strategi penguatan sistem keamanan siber di masa depan dapat disimpulkan ke berbagai seperti Karakteristik Teknologi Blockchain sebagai Fondasi Keamanan Digital yang dimana Teknologi *blockchain* memiliki karakteristik fundamental berupa desentralisasi, transparansi dan juga *immutability* yang menjadikannya sebagai sistem pencatatan digital dengan tingkat keamanan tergolong tinggi. Dengan tidak adanya otoritas tunggal, data yang tersimpan di dalam *blockchain* menjadi lebih sulit untuk dimanipulasi, diretas ataupun dihapus. Struktur kriptografis antarblok menciptakan lapisan keamanan yang mampu menjaga integritas data dan mencegah terjadinya perubahan tidak sah. Maka dari itu, *blockchain* berfungsi bukan hanya sebagai sistem penyimpanan informasi, tetapi juga sebagai mekanisme perlindungan data yang efektif untuk menunjang keamanan transaksi digital.

Peran Blockchain dalam Pencegahan Cybercrime pada Transaksi Digital
Pemanfaatan *blockchain* berperan signifikan dalam mengatasi berbagai bentuk kejahatan siber yang seringkali terjadi pada sistem keuangan dan transaksi elektronik di masyarakat luas. Melalui mekanisme konsensus kolektif dan enkripsi terdistribusi, setiap transaksi dalam jaringan *blockchain* diverifikasi secara otomatis oleh node-node independen sehingga sulit dimanipulasi oleh pihak yang tidak berwenang. Keberadaan *smart contract* turut memperkuat fungsi pencegahan dengan menghapus kebutuhan akan pihak ketiga serta meminimalisasi risiko penipuan, rekayasa sosial dan juga pelanggaran data. Dengan demikian, *blockchain* menjadi instrumen efektif untuk menciptakan sistem transaksi yang aman, transparan serta dapat dipercaya.

Agar potensi *blockchain* dapat dioptimalkan dalam mencegah *cybercrime*, diperlukan strategi yang bersifat kolaboratif dan berkelanjutan. Pemerintah di Indonesia perlu membangun kerangka regulasi adaptif yang mengakomodasi perkembangan teknologi desentralisasi tanpa menghambat inovasi. Industri keuangan dan teknologi diharapkan mengintegrasikan *blockchain* ke dalam sistem audit dan pengawasan internal guna memperkuat keamanan transaksi. Sementara itu juga, peningkatan literasi digital, riset akademik serta pengembangan infrastruktur nasional

menjadi persyaratan penting untuk memperluas penerapan *blockchain* di segala sektor. Sinergi antara pemerintah, industri, akademisi dan juga masyarakat membuat *blockchain* dapat menjadi dasar utama bagi sistem keamanan digital nasional yang tangguh, transparan dan juga berdaya saing secara global.

E. DAFTAR PUSTAKA

Jurnal

- Siahaan, P. Y., & Ng, J. (2024). Analisis implementasi teknologi *blockchain* dalam meningkatkan transparansi dan kepercayaan di sektor keuangan di Indonesia. *J. Sist. Inf. dan Ilmu Komput*, 2(4). Hlm. 09-31
- Lisdawati, L., Saputra, P. P., Yulianto, E., Lase, H., & Daryanto, D. (2024). Implementasi teknologi *blockchain* dalam akuntansi keuangan: Peluang dan tantangan bagi perusahaan di Indonesia. *Jurnal Neraca Peradaban*, 4(2), 152-158.
- Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi *Blockchain*: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, 2(1), 55-68.
- Hutabarat, S. A., Karina, I., Banjarnahor, J. W., ul Hosnah, A., & Asmarani, N. (2024). *Pengantar Hukum Pidana: Teori dan Implementasi pada Era Revolusi Industri 4.0 menuju Era Society 5.0*. PT. Sonpedia Publishing Indonesia. hlm. 4-5

Artikel/Situs Laman

- Aws.amazon. "Apa itu Teknologi *Blockchain*" <https://aws.amazon.com/id/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc> diakses 26 Oktober 2025
- Jagoan Hosting Team. "Node Adalah: Pengertian dan Fungsinya pada Jaringan Komputer" <https://www.jagoanhosting.com/blog/node-adalah/> diakses 26 Oktober 2025
- IBM. "Apa itu *blockchain*?" <https://www.ibm.com/id-id/topics/blockchain> diakses 26 Oktober 2025
- INDODAX ACADEMY. "Teknologi *Blockchain*" <https://indodax.com/academy/teknologi-blockchain/> diakses 26 Oktober 2025