INDOTECH
INDONESIAN JOURNAL OF EDUCATION AND COMPUTER SCIENCE

Indonesian Journal of Education And Computer Science

Vol. 2, No. 3, Desember 2024
Hal 172-180

E-ISSN : 2987-2650
P-ISSN : 2987-7644

Site : https://jurnal.intekom.id/index.php/indotech

Analisis Pengaruh Blockchain Terhadap Keamanan dan Privasi Sistem Pembayaran Kriptografi

Kelvin[1], Richard Raymond[2], Fahrur Rozzi Nasution [3], Andrew Law[4], Philisya Salim[5], Christin Christovany[6], Joosten[7]
[1,2,3,4,5,6,7] Fakultas Informatika, Universitas Mikroskil, Medan, Indonesia

Article Info

Article history:

Received Desember 18, 2024
Revised Desember 18, 2024
Accepted Desember 23, 2024

Kata Kunci:

Blockchain,
Sistem Pembayaran,
Privasi,
Keamanan Data,

Keywords:

Blockchain,
Payment Systems,
Privacy,
Data Security,

ABSTRAK

Teknologi blockchain, dengan karakteristiknya yang desentralisasi, transparan, dan tahan tamper, menawarkan solusi inovatif untuk mengatasi tantangan dalam sistem pembayaran tradisional. Dengan mekanisme konsensus seperti Proof of Work (PoW) dan Proof of Stake (PoS), blockchain dapat menjamin integritas data dan mencegah pengeluaran ganda. Keamanan transaksi terjaga melalui penggunaan kriptografi canggih, yang juga melindungi identitas pengguna. Meski demikian, implementasi blockchain menghadapi tantangan signifikan, termasuk skalabilitas, konsumsi energi, serta kompleksitas regulasi. Studi ini menganalisis pengaruh blockchain terhadap keamanan dan privasi dalam sistem pembayaran berbasis kriptografi, termasuk evaluasi teknik seperti Zero-Knowledge Proofs dan enkripsi homomorfik. Melalui pendekatan kualitatif berbasis analisis literatur dan studi kasus, penelitian ini mengeksplorasi aplikasi blockchain dalam berbagai sektor pembayaran, seperti pembayaran lintas batas dan micropayments, serta dampaknya terhadap peran lembaga keuangan. Hasilnya menunjukkan bahwa blockchain berpotensi meningkatkan efisiensi dan keamanan transaksi, meskipun isu regulasi dan privasi masih menjadi kendala utama untuk adopsi lebih luas.

ABSTRACT

Blockchain technology, with its decentralized, transparent, and tamper-resistant characteristics, offers innovative solutions to address challenges in traditional payment systems. Through consensus mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS), blockchain ensures data integrity and prevents double-spending. Transaction security is maintained using advanced cryptography, which also protects user identities. However, the implementation of blockchain faces significant challenges, including scalability, energy consumption, and regulatory complexity. This study analyzes the impact of blockchain on security and privacy in cryptography-based payment systems, including evaluations of techniques like Zero-Knowledge Proofs and homomorphic encryption. Through a qualitative approach based on literature analysis and case studies, the research explores blockchain applications in various payment sectors, such as cross-border payments and micropayments, as well as its impact on the role of financial institutions. The findings indicate that blockchain has the potential to enhance transaction efficiency and security, although regulatory and privacy issues remain major obstacles to broader adoption.

Corresponding Author:

Joosten
Fakultas Informatika, Universitas Mikroskil
Medan, Indonesia
Email: joosten.ng@mikroskil.ac.id

1. PENDAHULUAN

Revolusi digital telah membawa transformasi signifikan dalam berbagai sektor, termasuk industri keuangan. Salah satu inovasi paling menonjol adalah teknologi blockchain, yang menawarkan paradigma baru dalam pengelolaan data dan transaksi. Konsep blockchain yang terdesentralisasi, transparan, dan tahan tamper telah menarik minat yang besar, terutama dalam konteks sistem pembayaran berbasis kriptografi. [1], [2]

Teknologi blockchain memiliki potensi besar untuk meningkatkan keamanan dan privasi dalam transaksi keuangan. Dengan menggunakan kriptografi yang kuat dan mekanisme konsensus yang terdistribusi, blockchain dapat meminimalkan risiko penipuan, mengurangi biaya intermediasi, serta melindungi data pengguna dari akses yang tidak sah. [3], [4] Beberapa studi telah menunjukkan bahwa blockchain dapat meningkatkan efisiensi dan transparansi dalam proses verifikasi transaksi.[5]

Namun, implementasi blockchain dalam sistem pembayaran juga menghadirkan tantangan unik. Jenis blockchain yang berbeda, seperti public blockchain dan private blockchain, memiliki karakteristik keamanan dan privasi yang berbeda pula. Algoritma konsensus yang digunakan, seperti Proof of Work (PoW) dan Proof of Stake (PoS), juga memiliki implikasi yang signifikan terhadap kinerja dan keamanan sistem.[4] Selain itu, isu-isu terkait skalabilitas, interoperabilitas, dan regulasi masih perlu diatasi untuk memastikan adopsi blockchain yang lebih luas.[5]

Penelitian ini bertujuan untuk menganalisis secara mendalam pengaruh teknologi blockchain terhadap keamanan dan privasi pada sistem pembayaran berbasis kriptografi. Fokus utama penelitian ini adalah pada:

- Jenis-jenis blockchain: Membandingkan keamanan dan privasi yang ditawarkan oleh *public blockchain*, *private blockchain*, dan *hybrid blockchain* dalam konteks sistem pembayaran.[6]
- Algoritma konsensus: Menganalisis dampak berbagai algoritma konsensus, termasuk PoW, PoS, dan algoritma konsensus lainnya, terhadap keamanan dan efisiensi transaksi. [6], [7]
- Mekanisme privasi: Mengevaluasi penerapan teknik-teknik privasi seperti *zero-knowledge proofs* dan *homomorphic encryption* dalam meningkatkan kerahasiaan data pengguna.[6], [8]
- Kasus penggunaan: Menjelajahi berbagai kasus penggunaan blockchain dalam sistem pembayaran, seperti pembayaran lintas batas, micropayments, dan pembayaran dalam rantai pasok.[7]
- Dampak terhadap industri keuangan: Menganalisis potensi perubahan pada peran lembaga keuangan, intermediasi, dan inklusi keuangan sebagai akibat dari adopsi blockchain.[6], [7]

Dengan memahami secara komprehensif aspek-aspek di atas, penelitian ini diharapkan dapat memberikan kontribusi yang berharga bagi pengembangan sistem pembayaran yang lebih aman, efisien, dan inklusif.

2. METODE

Penilitian ini menggunakan pendekatan kualitatif dengan dua metode utama, yaitu analisis literatur dan studi kasus, untuk mendapatkan pemahaman mendalam tentang pengaruh teknologi blockchain terhadap keamanan dan privasi dalam sistem pembayaran.

Analisis literatur dilakukan dengan mengumpulkan dan mengkaji berbagai sumber akademis dan laporan industri yang relevan mengenai teknologi blockchain, keamanan data, privasi, dan implementasi sistem pembayaran. ang dimana mencakup membandingkan keamanan dan privasi yang ditawarkan oleh *public blockchain*, *private blockchain*, dan *hybrid blockchain* dalam konteks sistem pembayaran,

Menganalisis dampak berbagai algoritma konsensus, termasuk PoW, PoS, dan algoritma konsensus lainnya, terhadap keamanan dan efisiensi transaksi, serta Mengevaluasi penerapan teknik-teknik privasi seperti *zero-knowledge proofs* dan *homomorphic encryption* dalam meningkatkan kerahasiaan data pengguna.

Studi kasus diterapkan untuk menganalisis implementasi blockchain dalam sistem pembayaran di dunia nyata. Beberapa kasus yang dipilih mencakup aplikasi blockchain dalam pembayaran lintas batas, micropayments, dan sistem pembayaran dalam rantai pasok. Serta Menganalisis potensi perubahan pada peran lembaga keuangan, intermediasi, dan inklusi keuangan sebagai akibat dari adopsi blockchain.

Dengan menggunakan kedua metode ini, penelitian diharapkan dapat memberikan pandangan komprehensif tentang manfaat dan tantangan implementasi blockchain dalam sistem pembayaran serta dampaknya terhadap keamanan dan privasi transaksi.

3. HASIL DAN PEMBAHASAN

3.1 Analisis Keamanan dan Privasi pada Jenis-Jenis Blockchain

Teknologi *blockchain* telah muncul sebagai solusi inovatif dalam sistem pembayaran, menawarkan berbagai tingkat keamanan dan privasi berdasarkan jenisnya. Tiga kategori utama *blockchain* adalah *public blockchain, private blockchain*, dan *hybrid blockchain*. Masing-masing memiliki karakteristik unik yang mempengaruhi aspek keamanan dan privasi.

3.1.1 Public Blockchain

Public Blockchain adalah jenis blockchain yang terbuka untuk umum, di mana siapa saja dapat berpartisipasi dalam jaringan tanpa memerlukan izin. Dalam sistem ini, setiap individu dapat menjadi node, membaca, menulis, dan memperbarui informasi di blockchain dengan menggunakan alamat pribadi dan kunci publik. Public blockchain memiliki karakteristik transparansi yang tinggi, karena semua transaksi dapat dilihat oleh semua peserta jaringan, sehingga meningkatkan kepercayaan dan akuntabilitas. Contoh paling terkenal dari public blockchain adalah Bitcoin dan Ethereum, di mana semua transaksi dicatat secara permanen dan tidak dapat diubah oleh satu pihak pun.[9], [10], [11].

1. Keamanan

Public *blockchain*, seperti Bitcoin dan *Ethereum*, menawarkan tingkat keamanan yang tinggi melalui desentralisasi. Tidak ada titik kegagalan tunggal, sehingga sulit bagi penyerang untuk mengubah data tanpa menguasai lebih dari 50% dari seluruh *node* dalam jaringan (serangan 51%)[12], [13]. Selain itu, transaksi dicatat secara transparan, memungkinkan audit yang mudah oleh pengguna lain.

2. Privasi

Meskipun *public blockchain* menawarkan transparansi, privasi menjadi masalah. Transaksi bersifat *pseudonim*; alamat *wallet* dapat dihubungkan dengan identitas pengguna jika informasi tambahan tersedia[12] . Data sensitif yang disimpan dalam *smart contract* juga berisiko terpapar jika tidak dikelola dengan baik[12]

3.1.2 Private Blockchain

Private Blockchain adalah jenis blockchain yang hanya dapat diakses oleh entitas tertentu yang telah mendapatkan izin. Dalam private blockchain, akses untuk membaca dan menulis data dibatasi hanya kepada anggota yang telah divalidasi oleh pemilik jaringan. Hal ini memungkinkan kontrol yang lebih besar atas data dan privasi, sehingga cocok digunakan dalam lingkungan bisnis atau organisasi yang memerlukan keamanan tinggi. Private blockchain sering digunakan dalam aplikasi yang membutuhkan kerahasiaan dan efisiensi, seperti dalam industri perbankan atau perusahaan besar yang ingin mengelola data internal mereka dengan aman[10], [14].

1. Keamanan

Private blockchain, yang digunakan oleh perusahaan atau organisasi tertentu, memberikan kontrol lebih besar terhadap siapa yang dapat mengakses dan memvalidasi transaksi. Ini mengurangi risiko serangan eksternal karena hanya pihak-pihak tertentu yang memiliki akses ke jaringan[13], [15] . Namun, ketergantungan pada administrator pusat dapat menciptakan titik kegagalan jika tidak dikelola dengan baik.

2. Privasi

Private blockchain menawarkan privasi lebih baik dibandingkan *public blockchain*. Data transaksi tidak dapat diakses oleh publik, sehingga informasi sensitif tetap terlindungi. Pengguna memiliki kontrol lebih besar atas data mereka dan dapat menetapkan izin akses spesifik [13], [15].

3.1.3 Hybrid Blockchain

Hybrid Blockchain menggabungkan elemen dari public dan private blockchain. Dalam sistem ini, ada bagian dari blockchain yang bersifat publik, memungkinkan transparansi dan partisipasi umum, sementara bagian lainnya bersifat privat untuk menjaga kerahasiaan data sensitif. Hybrid blockchain memberikan fleksibilitas kepada organisasi untuk menggunakan keuntungan dari kedua jenis blockchain sesuai dengan kebutuhan mereka. Misalnya, sebuah perusahaan dapat menggunakan hybrid blockchain untuk membagikan informasi tertentu secara publik sambil menjaga data internal tetap aman dan terkendali[10], [16].

1. Keamanan

Hybrid blockchain menggabungkan elemen dari *public* dan *private blockchain*. Ini memungkinkan organisasi untuk memanfaatkan keamanan tinggi dari public blockchain sambil mempertahankan kontrol privasi dari *private blockchain*. Dengan struktur ini, organisasi dapat menentukan data mana yang bersifat publik dan mana yang harus tetap privat[13]**.**

2. Privasi

Hybrid blockchain menawarkan fleksibilitas dalam hal privasi. Data sensitif dapat disimpan secara privat sementara transaksi tertentu dapat dibagikan secara publik untuk transparansi. Ini memberikan keseimbangan antara transparansi dan perlindungan data pribadi[15].

3.2 Dampak Algoritma Konsensus terhadap Keamanan dan Efisiensi Transaksi

Algoritma konsensus merupakan elemen kunci dalam teknologi *blockchain*, berfungsi untuk memastikan keamanan dan keandalan transaksi dalam jaringan terdesentralisasi. Berbagai algoritma, seperti *Proof of Work* (PoW), *Proof of Stake* (PoS), dan varian lainnya, memiliki dampak yang signifikan terhadap kedua aspek ini.

3.2.1 Proof of Work (PoW)

Proof of Work (PoW) adalah mekanisme konsensus yang digunakan dalam sistem blockchain untuk memverifikasi transaksi dan menambang blok baru. Tujuan utama dari PoW adalah untuk mencegah serangan siber, seperti serangan *Distributed Denial of Service* (DDoS), yang dapat menghabiskan sumber daya sistem komputer dengan mengirimkan permintaan palsu. Dalam konteks *cryptocurrency* seperti Bitcoin, PoW berfungsi untuk memastikan bahwa setiap transaksi yang dilakukan adalah valid dan tidak ada pengguna yang dapat menghabiskan aset yang sama lebih dari sekali[17].

1. Keamanan:

PoW, yang digunakan oleh Bitcoin, menawarkan tingkat keamanan yang tinggi dengan memerlukan penambang untuk menyelesaikan masalah matematis kompleks. Hal ini membuat serangan terhadap

jaringan menjadi sangat mahal dan sulit dilakukan, karena penyerang harus menguasai lebih dari 50% dari daya komputasi jaringan untuk berhasil melakukan serangan ganda[18], [19] .

2. Efisiensi:

Namun, PoW juga memiliki kelemahan signifikan dalam hal efisiensi. Proses penambangan yang intensif energi menyebabkan waktu transaksi yang lebih lambat dan konsumsi energi yang tinggi. Ini menimbulkan kekhawatiran terkait keberlanjutan lingkungan dan biaya operasional[18], [20].

3.2.2 Proof of Stake (PoS)

Proof of Stake **(PoS)** adalah alternatif dari PoW yang dirancang untuk mencapai konsensus dalam jaringan blockchain tanpa memerlukan penggunaan energi komputasi yang besar. Dalam sistem PoS, validator dipilih untuk memverifikasi transaksi berdasarkan jumlah koin yang mereka miliki dan "taruhkan" dalam jaringan. Semakin banyak koin yang dimiliki oleh seorang validator, semakin besar kemungkinan mereka dipilih untuk memvalidasi blok baru[21].

1. Keamanan:

PoS berfungsi dengan memilih validator berdasarkan jumlah token yang mereka miliki, sehingga mengurangi kebutuhan akan daya komputasi yang besar. Meskipun PoS lebih ramah lingkungan, ada risiko terkait pemusatan kekuasaan di staking pool dan potensi serangan melalui "stake grinding," di mana validator berusaha untuk mendapatkan keuntungan tidak adil [18], [19].

2. Efisiensi

Dari segi efisiensi, PoS menawarkan kecepatan transaksi yang lebih baik dibandingkan dengan PoW. Dengan tidak memerlukan proses penambangan yang berat, PoS dapat memproses transaksi lebih cepat dan dengan konsumsi energi yang jauh lebih rendah[19], [20].

3.2.3 Algoritma Konsensus Lainnya

1. Byzantine Fault Tolerance (BFT): BFT dirancang untuk mencapai konsensus dengan cepat meskipun ada node yang berperilaku buruk. Ini memberikan keamanan tambahan dalam konteks di mana kecepatan transaksi sangat penting. Namun, BFT memerlukan sumber daya yang besar untuk beroperasi secara efektif[18], [20]

2. Directed Acyclic Graphs (DAGs): DAG menawarkan alternatif dengan memungkinkan transaksi diproses secara paralel, meningkatkan kecepatan dan skalabilitas. Namun, pendekatan ini tidak menjaga riwayat transaksi secara linier, yang dapat menimbulkan tantangan dalam hal auditabilitas dan keamanan data[18], [19].

3.3 Dampak Algoritma Konsensus terhadap Keamanan dan Efisiensi Transaksi

Teknologi *blockchain*, yang dikenal karena kemampuannya dalam menyediakan keamanan dan transparansi, juga menghadapi tantangan terkait privasi. Untuk meningkatkan kerahasiaan data pengguna, beberapa teknik privasi telah dikembangkan, termasuk *zero-knowledge proofs* dan *homomorphic encryption*. Evaluasi penerapan teknik-teknik ini penting untuk memahami efektivitasnya dalam menjaga privasi pengguna.

3.3.1 Zero-Knowledge Proofs (ZKP)

Zero-knowledge proofs, khususnya varian yang dikenal sebagai zk-SNARKs *(Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge)*, memungkinkan satu pihak untuk membuktikan kepada pihak lain bahwa suatu pernyataan benar tanpa mengungkapkan informasi tambahan tentang pernyataan tersebut. Dalam konteks blockchain, ZKP dapat digunakan untuk:

- Meningkatkan Anonimitas: ZKP memungkinkan transaksi dilakukan tanpa mengungkapkan identitas pengguna atau detail transaksi. Hal ini sangat penting dalam menjaga privasi pengguna di jaringan publik[22].

- Verifikasi Tanpa Pengungkapan: Pengguna dapat membuktikan kepemilikan aset atau memenuhi syarat tertentu tanpa harus mengungkapkan informasi sensitif yang relevan[23].

Penggunaan ZKP dalam blockchain telah menunjukkan potensi besar dalam meningkatkan privasi, meskipun implementasinya masih memerlukan penelitian lebih lanjut untuk mengoptimalkan efisiensi dan skalabilitas.

3.3.2 Homomorphic Encryption

Homomorphic Encryption adalah Teknik enkripsi yang memungkinkan operasi dilakukan pada data terenkripsi tanpa perlu mendekripsinya terlebih dahulu. Ini memberikan beberapa keuntungan:

- Pengolahan Data Terenkripsi: Dengan *Homomorphic Encryption,* data dapat diproses dan dianalisis tanpa pernah membongkar enkripsi, sehingga menjaga kerahasian informasi sensitif[24].
- Akses Terbatas: Hanya pihak yang memiliki kunci deskripsi yang dapat mengakses data asli setelah proses selesai. Ini memberikan kontrol lebih besar kepada pengguna atas siapa yang dapat melihat informasi mereka[23].

Meskipun *homomorphic encryption* menawarkan solusi menarik untuk privasi, tantangan utama terletak pada kompleksitas komputasi dan waktu pemrosesan yang lebih lama dibandingkan dengan metode tradisional.

3.3.3 Pseudonimitas dan Kontrol Akses

Dalam konteks *blockchain*, pseudonimitas merupakan fitur yang memungkinkan pengguna bertransaksi tanpa mengungkapkan identitas asli mereka. Meskipun alamat *blockchain* tidak langsung terkait dengan identitas pribadi, analisis dapat menghubungkan transaksi dengan individu tertentu jika informasi tambahan tersedia[22], [25]. Oleh karena itu, pengembangan teknik seperti mixnets juga penting untuk mencampurkan transaksi dari berbagai pengguna, sehingga menyulitkan pelacakan kembali ke individu tertentu. Selain itu, kontrol akses yang tepat juga menjadi aspek penting dalam menjaga privasi. Pengguna dapat memberikan izin akses kepada pihak lain untuk melihat atau menggunakan data mereka, dan dapat mencabut izin tersebut kapan saja[22].

3.4 Kasus Penggunaan Blockchain dalam Sistem Pembayaran

Blockchain telah menjadi solusi inovatif dalam sistem pembayaran, menawarkan berbagai manfaat, termasuk efisiensi, transparansi, dan keamanan. Beberapa kasus penggunaan utama dalam konteks ini mencakup pembayaran lintas batas, *micropayments*, dan pembayaran dalam rantai pasok.

3.4.1 Pembayaran Lintas batas

Pembayaran lintas batas adalah salah satu aplikasi paling signifikan dari teknologi *blockchain*. Dengan memanfaatkan *blockchain*, transaksi internasional dapat dilakukan secara langsung antara pihak yang terlibat tanpa perantara. Hal ini mengurangi biaya dan waktu yang diperlukan untuk menyelesaikan transaksi.

1. Keuntungan: *Blockchain* dapat menyelesaikan transaksi lintas batas dalam hitungan menit, dibandingkan dengan sistem tradisional yang memerlukan beberapa hari kerja[26]. Penelitian menunjukkan bahwa penerapan *blockchain* dapat mengurangi biaya transfer hingga 40%[26].

3.4.2 Micropayments

Micropayments adalah transaksi dengan nilai rendah yang sering kali tidak layak dilakukan melalui metode pembayaran tradisional karena biaya transaksi yang tinggi. *Blockchain* memungkinkan *micropayments* dengan biaya yang sangat rendah dan kecepatan transaksi yang tinggi.[26]

1. Keuntungan: Dengan biaya transaksi yang minimal, pengguna dapat melakukan pembayaran untuk layanan atau konten dengan nilai kecil, membuka peluang baru untuk model bisnis berbasis langganan mikro.

3.4.2 Pembayaran dalam Rantai Pasok

Blockchain juga digunakan untuk meningkatkan efisiensi dalam sistem pembayaran dalam rantai pasok. Dengan transparansi yang ditawarkan oleh teknologi ini, semua pihak dalam rantai pasok dapat memverifikasi transaksi secara langsung.

1. Keuntungan: Transparansi dan keamanan yang diberikan oleh *blockchain* membantu membangun kepercayaan antara pemasok dan pengecer, serta mempercepat proses pembayaran melalui penggunaan *smart contracts*[27], [28].

3.5 Dampak terhadap Industri Keuangan

Adopsi teknologi blockchain memiliki potensi untuk mengubah secara signifikan peran lembaga keuangan, intermediasi, dan inklusi keuangan. Berikut adalah analisis dampak tersebut berdasarkan referensi yang relevan.

3.5.1 Perubahan pada Peran Lembaga Keuangan

Blockchain memungkinkan transaksi finansial dilakukan secara langsung antara pihak-pihak yang terlibat tanpa memerlukan perantara seperti bank. Hal ini dapat mengurangi biaya transaksi dan meningkatkan efisiensi. Menurut penelitian, penggunaan blockchain dalam manajemen keuangan di perusahaan fintech telah menunjukkan bahwa teknologi ini memungkinkan transaksi yang lebih cepat, murah, dan aman, serta mengurangi risiko penipuan dan biaya administratif [29].

3.5.2 Intermediasi

Dengan adanya blockchain, peran lembaga keuangan sebagai perantara dalam transaksi dapat berkurang. Teknologi ini memungkinkan pencatatan dan verifikasi transaksi secara langsung oleh semua pihak yang terlibat, sehingga mengurangi ketergantungan pada lembaga tradisional. Penelitian menunjukkan bahwa blockchain dapat menciptakan sistem pembayaran yang lebih efisien dan transparan, serta meningkatkan aksesibilitas layanan keuangan bagi individu yang sebelumnya terpinggirkan[30].

3.5.3 Inklusi Keuangan

Blockchain berpotensi meningkatkan inklusi keuangan dengan memberikan akses kepada individu yang tidak memiliki rekening bank untuk berpartisipasi dalam sistem keuangan. Cryptocurrency dan teknologi berbasis blockchain memungkinkan pengguna untuk melakukan transaksi tanpa memerlukan rekening bank tradisional. Ini sangat penting di negara-negara berkembang di mana akses ke layanan keuangan masih terbatas. Penelitian menunjukkan bahwa adopsi teknologi ini dapat membuka peluang baru untuk pertumbuhan bisnis dan akses keuangan yang lebih luas bagi masyarakat [29] [31]

4. KESIMPULAN

Public blockchain menawarkan keamanan tinggi melalui desentralisasi, namun menghadapi tantangan dalam privasi karena sifat transparansinya. Private blockchain memberikan kontrol yang lebih baik terhadap privasi, tetapi rentan terhadap kegagalan pada titik sentral. Hybrid blockchain mampu memberikan keseimbangan antara keamanan dan privasi, menjadikannya pilihan yang menarik dalam berbagai kasus penggunaan.

Algoritma konsensus seperti Proof of Work (PoW) dan Proof of Stake (PoS) memiliki keunggulan dan kekurangan masing-masing. PoW menawarkan keamanan tinggi tetapi tidak efisien secara energi, sedangkan PoS lebih efisien tetapi menghadapi risiko pemusatan kekuasaan. Algoritma alternatif seperti Byzantine Fault Tolerance (BFT) dan Directed Acyclic Graphs (DAGs) menghadirkan peluang untuk meningkatkan skalabilitas dan kecepatan transaksi.

Penerapan teknik seperti zero-knowledge proofs (ZKP) dan homomorphic encryption menunjukkan potensi besar dalam melindungi kerahasiaan data pengguna. Namun, implementasi teknik ini masih menghadapi tantangan terkait efisiensi dan kompleksitas komputasi.

Blockchain telah membuktikan nilai praktisnya dalam sistem pembayaran lintas batas, micropayments, dan pembayaran dalam rantai pasok. Keuntungan utama mencakup pengurangan biaya transaksi, peningkatan efisiensi, dan transparansi.

Adopsi blockchain berpotensi mengurangi peran lembaga keuangan tradisional sebagai perantara, mengubah model intermediasi, dan mendorong inklusi keuangan. Teknologi ini membuka akses ke layanan keuangan bagi masyarakat yang tidak memiliki akses ke sistem perbankan konvensional, terutama di negara berkembang.

REFERENSI

[1] Z. Xie, S. Dai, H.-N. Chen, dan X. Wang, “Blockchain challenges and opportunities: a survey,” 2018.
[2] V. Gugueoth, S. Safavat, S. Shetty, dan D. Rawat, “A review of IoT security and privacy using decentralized blockchain techniques,” 1 November 2023, *Elsevier Ireland Ltd*. doi: 10.1016/j.cosrev.2023.100585.
[3] Untung Raharfja, Qurtul Aini, M. Yusup, dan Aulia Edliyanti, “Penerapan Teknologi Blockchain Sebagai Media Pengamanan Proses Transaksi E-Commerce,” 2020.
[4] Buntoro Irawan, “Humantech Jurnal Ilmiah Multi Disiplin Indonesia Implementasi Teknologi Blockchain Untuk Keamanan Data Internet Of Things,” 2023.
[5] M. Bahanan, S. Al-Utsmani Bondowoso, dan M. Wahyudi, “Analisis Pengaruh Penggunaan Teknologi Blockchain Dalam Transaksi Keuangan Pada Perbankan Syariah,” 2023.
[6] V. Buterin, J. Illum, M. Nadler, F. Schär, dan A. Soleimani, “Blockchain privacy and regulatory compliance: Towards a practical equilibrium,” *Blockchain: Research and Applications*, vol. 5, no. 1, Mar 2024, doi: 10.1016/j.bcra.2023.100176.
[7] B. Ram dan P. Verma, “Application of blockchain technology in data security,” *IP Indian Journal of Library Science and Information Technology*, vol. 9, no. 1, hlm. 51–55, Agu 2024, doi: 10.18231/j.ijlsit.2024.008.
[8] P. Khordadpour dan S. Ahmadi, “Security and Privacy Enhancing in Blockchain-based IoT Environments via Anonym Auditing,” 2024.
[9] Teguh Prasetyo Utomo, “Implementasi Teknologi Blockchain Di Perpustakaan : Peluang, Tantangan Dan Hambatan,” *Buletin Perpustakaan Universitas Islam Indonesia*, vol. 4, no. 2, hlm. 173–200, 2021.
[10] M. Oka Augusta, C. Putriana Oktaviandi Syeira, A. Hadiapurwa, dan K. Kunci, “Penggunaan Teknologi Blockchain Dalam Bidang Pendidikan,” vol. 437, no. 2, 2021, [Daring]. Tersedia pada: https://digitalcredentials.mit.edu
[11] A. Winarno, “Desain E-Transkrip Dengan Teknologi Blockchain,” 2019. [Daring]. Tersedia pada: https://followmyvote.com/online-voting-technology/blockchain-technology/
[12] Willy Kristian, “Privacy and Security Concern in Blockchain,” BINUS UNIVERSITY. Diakses: 17 Desember 2024. [Daring]. Tersedia pada: https://sis.binus.ac.id/2024/01/18/privacy-and-security-concern-in-blockchain/
[13] R. Setianingsih, U. I. Negeri, dan 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, hlm. 3047–9673, 2024, doi: 10.61722/jinu.v1i4.1841.
[14] A. Fuadi Tanjung dan P. Wati, “Penerapan Teknologi Blockchain Dalam Akuntansi Syariah,” vol. 8, 2023, doi: 10.30651/jms.v8i2.19282.

[15] Tito Wira Eka Suryawijaya, "Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia," vol. 2, no. 1, hlm. 55–67, 2023, doi: 10.21787/jskp.2.2023.55-67.
[16] "Blockchain: Pengertian, Manfaat, dan Cara Kerjanya," Binus University Online.
[17] Willy Kristian, "Pengertian Konsep Proof of Work pada Cryptocurrency," Binus University. Diakses: 18 Desember 2024. [Daring]. Tersedia pada: https://sis.binus.ac.id/2021/10/15/pengertian-konsep-proof-of-work-pada-cryptocurrency/
[18] Drajad Wiryawan, "Analisis Mendalam tentang Keamanan Mekanisme Konsensus dalam Teknologi Blockchain," Binus University. Diakses: 17 Desember 2024. [Daring]. Tersedia pada: https://sis.binus.ac.id/2024/06/25/analisis-mendalam-tentang-keamanan-mekanisme-konsensus-dalam-teknologi-blockchain/
[19] Willy Kristian, "Peran Algoritma Konsensus dalam Jaringan Blockchain," Binus University. Diakses: 17 Desember 2024. [Daring]. Tersedia pada: https://sis.binus.ac.id/2024/01/26/peran-algoritma-konsensus-dalam-jaringan-blockchain/
[20] Eleazer Gottlieb Julio Sumampouw dan Irwan Sembiring, "Analisis Verifikasi Proof Of Stake (Pos) Nft Dengan Teknologi Smart Contract," 2024.
[21] D. Irawan, "Mekanisme Prof Of Work (Pow) Dan Delegated Proof Of Stake (Dpos) Untuk Maksimalisasi Keamanan, Skalabilitas, Dan Desentralisasi," vol. 4, no. 1, hlm. 68–75, 2023.
[22] Felicia, Elvilie, Calista, Sebastian Areen Chic, Muhammad Fardian Bilqisthi, dan Joosten, "Tantangan dan Peluang Blockchain di Era Digital dalam Bidang Keamanan Data dan Transaksi Digital," 2024.
[23] S. Afdilah, N. S. Agustina, I. Hani, dan I. Gunawan, "Penerapan Teknologi Blockchain dalam Meningkatkan Keamanan Sistem Identifikasi Pengguna," *Journal Shift Vol*, vol. 4, 2024.
[24] G. R. Nabilla, "Tren Keamanan Informasi berbasis Blockchain di Masa Kini dan di Masa Mendatang," 2023. [Daring]. Tersedia pada: https://www.researchgate.net/publication/370073770
[25] Willy Kristian, "Privasi Blockchain: Apakah Data Anda Masih Pribadi atau Telah Menjadi Umum?," Binus University. Diakses: 18 Desember 2024. [Daring]. Tersedia pada: https://binus.ac.id/bekasi/2024/07/privasi-blockchain-apakah-data-anda-masih-pribadi-atau-telah-menjadi-umum/
[26] R. Mustaqim Handoko, B. Aulyansyah Ahmad Trisna, R. Delon Pratama, dan J. Parhusip, "Implementasi Blockchain Untuk Keamanan Sistem Pembayaran Digital dan Optimasi Transaksi Keuangan (Studi Kasus Industri Fintech di Indonesia)," *Jurnal Ilmu Teknik dan Informatika*, vol. 4, hlm. 64–74, doi: 10.51903/teknik.
[27] M. Bahanan, S. Al-Utsmani Bondowoso, dan M. Wahyudi, "Analisis Pengaruh Penggunaan Teknologi Blockchain Dalam Transaksi Keuangan Pada Perbankan Syariah."
[28] L. Megawati, C. Wiharma, dan A. Hasanudin, "Peran Teknologi Blockchain Dalam Meningkatkan Keamanan Dan Kepastian Hukum Dalam Transaksi Kontrak Di Indonesia," Online, 2023. [Daring]. Tersedia pada: https://jurnal.unsur.ac.id/jmj
[29] I. Ariati dan D. Rudianto, "Dampak Blockchain dalam Manajemen Keuangan pada Perusahaan Fintech," *Journal of Economics and Business UBS*, 2024.
[30] Steven Agustianto, "Pengaruh Kehadiran Blockchain dan Cryptocurrency Terhadap Masa Depan Industri Keuangan," Binus University. Diakses: 18 Desember 2024. [Daring]. Tersedia pada: https://sis.binus.ac.id/2024/02/22/pengaruh-kehadiran-blockchain-dan-cryptocurrency-terhadap-masa-depan-industri-keuangan/
[31] S. Jam dan G. Made Dwi Praditya Rahadi, "Dampak Teknologi Blockchain pada Sistem Pengendalian Internal Perusahaan di Sektor Keuangan," *Jurnal Cendekia Ilmiah*, vol. 3, no. 4, 2024.