JCS Journal of Comprehensive Science
JOURNAL OF COMPREHENSIVE SCIENCE
Published by Green Publisher
Crossref Google Scholar GARUDA PKP|INDEX

Journal of Comprehensive Science
p-ISSN: 2962-4738 e-ISSN: 2962-4584
Vol. 3. No. 11 November 2024

Tantangan dan Peluang Blockchain di Era Digital dalam Bidang Keamanan Data dan Transaksi Digital

Felicia[1*], Elvilie[2], Calista[3], Sebastian Areen Chic[4], Muhammad Fardian Bilqisthi[5], Joosten[6]
Universitas Mikroskil, Medan , Indonesia[1,2,3,4,5,6]
Email: 211121667@students.mikroskil.ac.id[1*], 211122018@students.mikroskil.ac.id[2], 211120544@students.mikroskil.ac.id[3], 211121456@students.mikroskil.ac.id[4], 211121837@students.mikroskil.ac.id[5], joosten.ng@mikroskil.ac.id[6]

Abstrak

Era digital telah mengubah cara kita berinteraksi, melakukan transaksi, dan menyimpan data. Namun, tantangan keamanan terkait data dan transaksi kini semakin mendesak. Kejahatan siber yang semakin canggih mengancam integritas dan kepercayaan terhadap sistem digital. Teknologi blockchain, yang bersifat terdesentralisasi dan mencatat transaksi secara permanen dan transparan, muncul sebagai solusi yang menjanjikan. Artikel ini akan membahas potensi blockchain dalam meningkatkan keamanan data dan transaksi di masa depan. Kita akan mengulas bagaimana blockchain membangun sistem yang aman dengan data yang terdistribusi dan terenkripsi, sehingga sulit untuk diubah atau diretas. Teknologi ini mendukung transaksi yang terverifikasi dan tidak dapat dipalsukan, yang pada gilirannya mengurangi risiko penipuan dan meningkatkan kepercayaan dalam sistem keuangan. Blockchain dianggap sebagai langkah penting dalam melindungi infrastruktur digital dan informasi sensitif. Dengan fitur desentralisasi, transparansi, dan kriptografi yang kuat, blockchain menawarkan keamanan tingkat tinggi yang sulit untuk dimanipulasi. Artikel ini mengulas potensi blockchain dalam meningkatkan keamanan data dan transaksi, serta tantangan yang perlu diatasi. Ditemukan bahwa blockchain memberikan keamanan tingkat tinggi melalui desentralisasi, transparansi, dan kriptografi yang kuat. Selain itu, blockchain menawarkan efisiensi, otomatisasi melalui smart contracts, dan potensi penerapan luas di berbagai sektor. Meskipun terdapat keterbatasan dan tantangan, upaya kolaboratif dan inovasi terus menerus dapat memperkuat peran blockchain dalam mengamankan data dan transaksi di masa depan. Diharapkan, artikel ini memberikan pemahaman yang lebih mendalam tentang peran blockchain dalam menghadapi tantangan keamanan digital saat ini dan di masa depan, serta bagaimana teknologi ini dapat membantu menciptakan lingkungan digital yang lebih aman dan terpercaya.

Kata Kunci: blockchain, keamanan data, kejahatan siber, transparansi, transaksi

Abstract

The digital era has changed the way we interact, conduct transactions, and store data. However, the security challenges related to data and transactions are now becoming more pressing. Cybercrime becoming increasingly sophisticated threatens the integrity and trust in digital systems. Blockchain technology, which is decentralized and records transactions permanently and transparently, has emerged as a promising solution. This article will discuss the potential of blockchain in enhancing data and transaction security in the future. We will review how blockchain builds a secure system with distributed and encrypted data, making it

difficult to alter or hack. This technology supports verified and tamper-proof transactions, which in turn reduces the risk of fraud and increases trust in the financial system. Blockchain is considered an important step in protecting digital infrastructure and sensitive information. With features of decentralization, transparency, and strong cryptography, blockchain offers a high level of security that is difficult to manipulate. This article reviews the potential of blockchain in enhancing data and transaction security, as well as the challenges that need to be addressed. It was found that blockchain provides high-level security through decentralization, transparency, and strong cryptography. In addition, blockchain offers efficiency, automation through smart contracts, and the potential for widespread application across various sectors. Although there are limitations and challenges, collaborative efforts and continuous innovation can strengthen the role of blockchain in securing data and transactions in the future. It is hoped that this article provides a deeper understanding of the role of blockchain in addressing current and future digital security challenges, as well as how this technology can help create a safer and more trustworthy digital environment.

Keywords: *blockchain, data security, cybercrime, transparency, transactions*

PENDAHULUAN

Perkembangan teknologi digital telah menghadirkan perubahan besar dalam hampir semua aspek kehidupan manusia. Kita hidup di era di mana informasi mengalir dengan cepat, transaksi dapat dilakukan dengan mudah, dan penyimpanan data menjadi lebih efisien. Akses informasi yang lebih mudah, proses transaksi yang lebih cepat, dan penyimpanan data yang lebih efisien telah mengubah cara kita berinteraksi, berbisnis, dan bahkan bermasyarakat. Namun, di balik kemajuan pesat ini, terdapat tantangan yang tidak kalah pentingnya, yaitu keamanan data dan transaksi. Kejahatan siber yang semakin canggih dan terorganisir mengancam integritas data dan kepercayaan dalam sistem digital. Pencurian data, pemalsuan identitas, serangan *ransomware*, dan berbagai bentuk kejahatan siber lainnya telah menjadi ancaman nyata yang dapat merugikan individu, organisasi, dan bahkan negara.

Dalam beberapa cara, teknologi blockchain dapat meningkatkan keamanan data. Pertama, karena memungkinkan data disimpan secara terdesentralisasi dan terenkripsi, data lebih aman. Dengan menggunakan kriptografi yang kuat dan algoritma konsensus yang terdesentralisasi, *blockchain* dapat memberikan lapisan perlindungan tambahan terhadap serangan siber seperti peretasan dan modifikasi data yang tidak sah (Setianingsih & Nasution, 2024).

Lapisan keamanan yang tak tertandingi, menjadikan data yang disimpan di dalamnya sulit diakses atau dimodifikasi oleh pihak yang tidak berwenang(RISHKA). Karena data tidak disimpan secara sentral, orang tidak dapat mencuri atau mengubah data tanpa persetujuan seluruh jaringan *blockchain*. Kedua, dalam teknologi *blockchain*, setiap transaksi dan data dapat diverifikasi oleh semua pihak yang terlibat. Hal ini meningkatkan transparansi dan mengurangi resiko penipuan. Ketiga, proses verifikasi dan validasi dalam teknologi *blockchain* sangat efisien dan cepat, karena tidak memerlukan perantara atau pihak ketiga (Suryawijaya, 2023). *Blockchain*, sebagai teknologi terdesentralisasi yang mencatat transaksi secara permanen dan transparan, muncul sebagai solusi potensial untuk mengatasi tantangan ini. Dengan mendistribusikan data dan menggunakan enkripsi yang kuat, *blockchain* menciptakan sistem yang lebih aman dan transparan, sehingga sulit untuk diubah atau diretas. Teknologi ini juga memungkinkan transaksi yang terverifikasi dan tidak dapat dipalsukan serta mengurangi resiko penipuan.

Menurut Madya et al., (2023) pencurian data, pemalsuan identitas, dan serangan siber lainnya menjadi ancaman nyata yang dapat merugikan individu, organisasi, dan bahkan negara. Data pribadi kita, yang tersimpan di berbagai *platform* digital, rentan terhadap pencurian dan penyalahgunaan. Transaksi keuangan *online*, yang semakin marak, juga menjadi sasaran empuk para penjahat siber. Di tengah ancaman yang semakin kompleks ini, *blockchain* muncul

sebagai solusi potensial untuk meningkatkan keamanan dan kepercayaan dalam dunia digital. *Blockchain*, sebuah teknologi terdesentralisasi yang mencatat transaksi secara permanen dan transparan, menawarkan cara baru untuk mengamankan data dan transaksi.

Bayangkan sebuah sistem pembayaran digital yang menggunakan *blockchain*. Setiap transaksi tercatat secara permanen dan dapat diverifikasi oleh semua pihak yang terlibat. Ini menghilangkan risiko penipuan dan manipulasi, karena setiap perubahan pada catatan transaksi akan terlihat oleh semua orang. Atau bayangkan sebuah sistem rantai pasokan yang menggunakan *blockchain* untuk melacak pergerakan barang secara *real-time,* dari produsen hingga konsumen. Dengan *blockchain*, setiap tahap dalam rantai pasokan dapat direkam dan diverifikasi, sehingga meningkatkan transparansi dan mengurangi risiko pemalsuan atau pencurian (Kiki Kristanto et al., 2024).

Meskipun menawarkan solusi yang menjanjikan, *blockchain* masih menghadapi beberapa tantangan. Skalabilitas *blockchain*, kemampuannya untuk menangani volume transaksi yang besar, masih menjadi kendala. Regulasi yang belum jelas tentang *blockchain* juga menghambat pengembangan dan penerapan teknologi ini. Peningkatan edukasi dan sosialisasi tentang *blockchain* sangat penting untuk mendorong adopsi pengguna. Tidak menutup kemungkinan adanya serangan yang berhasil menembus sistem keamanannya (Hendrayana et al., 2024). Namun, tantangan seperti skalabilitas teknologi dan ketidakteraturan regulasi masih menjadi hambatan yang perlu diatasi agar implementasi teknologi ini dapat sukses secara menyeluruh (analisis teknologi blockchain).

Beberapa jenis serangan yang dapat terjadi pada *blockchain* antara lain serangan *51% attack, double-spending attack, sybil attack,* dan lain-lain. Serangan *51% attack* terjadi ketika seorang penyerang berhasil menguasai lebih dari 50% kekuatan jaringan *blockchain* (Trinowo, 2020). Dengan menguasai lebih dari 50% kekuatan jaringan, penyerang dapat memalsukan transaksi dan mengganti catatan transaksi yang telah dilakukan sebelumnya. Hal ini dapat merusak integritas data dan mengancam keamanan data dalam *blockchain*. *Double-spending attack* adalah serangan di mana seorang penyerang mencoba untuk melakukan transaksi yang sama dua kali menggunakan aset kripto yang sama.

Sistem pembayaran digital juga rentan terhadap penipuan. *Blockchain* dapat meningkatkan keamanan transaksi karena setiap transaksi dicatat di *blockchain* dan dilacak, mengurangi risiko penipuan dan meningkatkan transparansi. Bank Indonesia sedang mengembangkan sistem pembayaran digital berbasis *blockchain* untuk meningkatkan efisiensi dan keamanan transaksi. Teknologi seperti *blockchain* dapat meningkatkan transparansi dan akuntabilitas dalam operasi bank sentral. Dengan blockchain, transaksi dapat dicatat secara permanen dan transparan, mengurangi risiko manipulasi serta meningkatkan kepercayaan publik terhadap sistem keuangan (Hidayat et al., 2023).

Berdasarkan data *United Nations Conference on Trade and Development* (UNCTAD) tahun 2015, menyebutkan terdapat 2.100 kasus yang menimbulkan permasalahan terkait data pribadi milik pengguna *e-commerce* dengan jumlah mencapai 822 juta data pribadi terekam dalam kegiatan *e-commerce*, serta dikumpulkan di *marketplace* (Nugroho et al., 2021). Kemudian, terdapat 152 juta data pribadi, seperti nama, enkripsi *password*, identitas konsumen, nomor kartu kredit dan debit, serta berbagai informasi yang berkaitan dengan data pembelian konsumen. Pihak yang melakukan pelanggaran data pribadi dengan tujuan untuk kepentingan bisnis sekitar 53% pelaku usaha. Dengan penerapan teknologi blockchain pada proses transaksi di *marketplace*, diharapkan dapat meningkatkan kepercayaan pembeli dalam melakukan transaksi secara langsung melalui internet, sehingga terjalin hubungan baik dan saling percaya antara penjual dan pembeli. Kepercayaan ini tidak hanya dijamin oleh perusahaan, tetapi juga didukung oleh kolaborasi antara kriptografi dan kode pintar (anggit panji) (Herlina et al., 2023).

Dalam *blockchain*, setiap transaksi harus diverifikasi dan disetujui oleh seluruh jaringan. Namun, dalam *double-spending attack*, penyerang mencoba untuk memalsukan transaksi dan

mengirimkan aset kripto yang sama ke dua alamat yang berbeda secara bersamaan. Hal ini dapat mengakibatkan kerugian finansial yang signifikan bagi pihak yang menerima aset kripto tersebut. *Sybil Attack* adalah serangan di mana seorang penyerang mencoba untuk mengambil alih jaringan *blockchain* dengan membuat banyak identitas palsu. Dalam *sybil attack*, penyerang membuat banyak identitas palsu yang tampaknya berasal dari banyak node jaringan yang berbeda. Hal ini dapat membuat penyerang memiliki kekuatan yang lebih besar dalam jaringan dan dapat memalsukan transaksi dan data (Suryawijaya, 2023).

Blockchain, yang pertama kali dikenal sebagai infrastruktur di balik mata uang digital seperti Bitcoin, sekarang telah berkembang menjadi lebih dari sekadar itu. Konsep dasarnya, yaitu desentralisasi, keamanan kriptografi, dan transparansi, membuka pintu bagi berbagai aplikasi di luar dunia keuangan (Damanik & Nasution, 2024). *Blockchain* menawarkan peluang besar dengan potensinya yang luar biasa untuk meningkatkan kepercayaan dalam sistem digital. Untuk mengatasi masalah ini, peluang terdapat dalam membangun kerjasama dengan penyedia *cyber security* dan pakar di bidang keamanan dan privasi data untuk meningkatkan perlindungan data pengguna (Hildawati et al., 2024). Teknologi ini memberikan kemampuan untuk menciptakan catatan transaksi yang bersifat permanen, transparan, dan sulit untuk diubah, yang membuatnya ideal untuk sistem yang memerlukan integritas dan keamanan tinggi. Dengan adanya *blockchain*, setiap transaksi yang tercatat menjadi bagian dari jaringan yang diamankan melalui proses kriptografi canggih, sehingga hampir tidak mungkin untuk dimanipulasi. Salah satu manfaat utama penerapan *blockchain* dalam pengelolaan keamanan data adalah peningkatan keandalan (Dhanu Prayogo et al., 2022). Hal ini menjadikan *blockchain* sebagai teknologi yang sangat andal dalam mencegah kecurangan atau perubahan data yang tidak sah, serta memungkinkan audit dan pelacakan yang efisien.

Di sektor keuangan, *blockchain* membawa peluang untuk menghilangkan perantara dalam berbagai transaksi, yang selama ini menambah biaya dan waktu (Djumadi, 2024). Dengan mekanisme *peer-to-peer* yang dimungkinkan oleh *blockchain*, proses keuangan seperti transfer uang lintas negara, pinjaman, dan manajemen aset dapat menjadi lebih cepat, transparan, dan hemat biaya. Tidak hanya itu, *blockchain* juga mengurangi ketergantungan pada institusi perbankan tradisional, sehingga menciptakan inklusi keuangan yang lebih baik, terutama di wilayah yang kurang terlayani oleh sistem perbankan formal (Tuna, 2024).

Blockchain juga memainkan peran penting, salah satunya melalui *Ripple* (XRP), yang membantu proses transaksi lintas batas antar bank serta institusi keuangan. Proses transaksi internasional melalui sistem perbankan tradisional biasanya memakan waktu berhari-hari dan membutuhkan biaya yang cukup tinggi. *Ripple* dengan teknologinya memanfaatkan *blockchain* untuk mengatasi hambatan ini, membuat transaksi lebih cepat dan murah karena dapat menghilangkan perantara. Namun, *Ripple* menghadapi tantangan besar dari sisi regulasi, terutama di Amerika Serikat terkait klasifikasi XRP sebagai sekuritas, yang menjadi penghalang adopsi massal dan menunjukkan tantangan regulasi dalam penerapan *blockchain* di sektor keuangan.

Seiring perkembangan teknologi dan meningkatnya kesadaran masyarakat tentang pentingnya keamanan data, implementasi *blockchain* di berbagai bidang terus meningkat. Teknologi ini diyakini akan memainkan peran penting dalam membentuk masa depan keamanan data dan transaksi di era digital. Ke depan, kita dapat membayangkan dunia yang lebih aman, transparan, dan terpercaya, di mana teknologi *blockchain* tidak hanya menjadi fondasi sistem keuangan dan ekonomi digital yang stabil, tetapi juga mendorong inovasi di berbagai bidang lainnya. Artikel ini mengkaji potensi *blockchain* dalam meningkatkan keamanan data dan transaksi di masa depan. Melalui pemahaman mendalam tentang konsep *blockchain* dan analisis terhadap berbagai penerapannya, artikel ini akan memberikan gambaran yang lebih jelas tentang bagaimana teknologi ini dapat mengubah masa depan keamanan data dan transaksi di era digital.

Artikel ini akan mengulas secara mendalam berbagai aspek penting dari teknologi *blockchain*, mencakup mekanisme kerjanya, keunggulan-keunggulannya dalam meningkatkan keamanan data, serta potensinya dalam mendukung transaksi keuangan yang lebih transparan, cepat, dan efisien. *Blockchain* adalah teknologi buku besar terdesentralisasi yang memungkinkan setiap transaksi dicatat dengan aman dalam jaringan yang tersebar luas, tanpa memerlukan perantara seperti institusi keuangan tradisional (Chairunnas et al., 2024). Artikel ini akan menjelaskan bagaimana mekanisme *blockchain* beroperasi melalui proses verifikasi oleh konsensus jaringan, yang menciptakan catatan transaksi yang bersifat permanen dan sulit untuk dimanipulasi. Selain itu, artikel ini akan mengeksplorasi keunggulan *blockchain* dalam meningkatkan keamanan data. Melalui sistem enkripsi yang kompleks dan struktur data yang tidak mudah diubah, *blockchain* memberikan tingkat keamanan yang sangat tinggi terhadap risiko kebocoran data dan kecurangan. Teknologi ini memiliki potensi besar dalam melindungi berbagai jenis data, termasuk data pribadi, data kesehatan, serta data sensitif lainnya, karena setiap perubahan yang dilakukan pada jaringan *blockchain* memerlukan persetujuan dari mayoritas node yang terlibat.

Di sektor keuangan, *blockchain* telah banyak diadopsi dalam transaksi lintas batas, pengelolaan aset, dan sektor pembayaran digital. Artikel ini akan mengupas bagaimana blockchain mampu menghilangkan perantara dan mempercepat proses transaksi, sekaligus mengurangi biaya yang terkait dengan proses transaksi internasional. Dengan semakin banyaknya aplikasi *blockchain* dalam pembayaran digital, teknologi ini juga berpotensi mengubah cara kita melakukan transaksi sehari-hari, memberikan kesempatan bagi sistem keuangan yang lebih inklusif dan efisien. Di sisi lain, artikel ini tidak hanya menyoroti keunggulan *blockchain* tetapi juga tantangan-tantangan yang dihadapi teknologi ini dalam mencapai adopsi massal. Beberapa tantangan signifikan yang dibahas dalam artikel ini meliputi skala jaringan yang terbatas, konsumsi energi tinggi, dan kebutuhan akan regulasi yang sesuai. Meskipun *blockchain* menawarkan transparansi dan keamanan yang tinggi, penerapannya dalam skala besar memerlukan pemecahan tantangan-tantangan ini agar teknologi dapat berjalan secara optimal dan tidak membebani infrastruktur digital.

Dengan analisis yang komprehensif, artikel ini bertujuan untuk memberikan pemahaman yang lebih baik tentang potensi *blockchain* dalam mengatasi berbagai tantangan keamanan data dan transaksi di era digital. Di samping membahas penerapan *blockchain* dalam berbagai sektor, artikel ini juga akan menyoroti aspek-aspek penting yang perlu dipertimbangkan dalam pengembangan dan penerapan teknologi *blockchain* di masa depan. Dengan demikian, artikel ini diharapkan dapat memberikan wawasan yang berharga bagi para pembaca tentang arah perkembangan *blockchain* ke depan, sekaligus menawarkan pandangan kritis mengenai peluang yang terbuka dan hambatan yang mungkin dihadapi oleh teknologi ini di berbagai sektor.

METODE PENELITIAN

Metode yang dipakai dalam penelitian ini berupa studi literatur. Studi literatur yang dilakukan di sini merupakan pengumpulan referensi seperti buku, jurnal, artikel, dan lain sebagainya. Tahapan dalam penelitian dengan metode ini yaitu dilakukan pencarian dan penentuan topik atau judul yang akan digunakan terlebih dahulu, lalu mencari referensi dari topik tersebut, setelah itu kumpulkan referensi-referensinya, dan mulai melakukan evaluasi dari kualitas referensi yang didapatkan. Tahap selanjutnya adalah mengkaji referensi yang telah dievaluasi tersebut, dan menulis hasil kajiannya di laporan penelitian. Penelitian ini dimulai dengan menentukan topik dan judul penelitian yang spesifik dan terfokus. Proses ini melibatkan identifikasi area penelitian yang menarik, relevan, dan memiliki potensi untuk menghasilkan kontribusi baru terhadap bidang ilmu pengetahuan. Pemilihan topik dan judul yang tepat menjadi pondasi yang kuat bagi seluruh proses penelitian. Setelah topik dan judul

penelitian ditetapkan, langkah selanjutnya adalah pencarian referensi yang relevan dan kredibel. Proses pencarian referensi melibatkan penggunaan berbagai sumber, seperti perpustakaan, *database online,* dan mesin pencari. Referensi-referensi yang ditemukan kemudian dikumpulkan, baik dengan membaca langsung, mencetak, maupun menyimpan secara digital.

Setelah referensi terkumpul, langkah selanjutnya adalah melakukan evaluasi terhadap kualitas referensi yang didapatkan. Evaluasi ini bertujuan untuk memastikan bahwa referensi yang digunakan memiliki kredibilitas, relevansi, dan akurasi yang tinggi. Tahap selanjutnya adalah mengkaji referensi yang telah dievaluasi tersebut. Proses kajian ini dilakukan dengan membaca, mencatat, dan menginterpretasi informasi yang relevan dengan topik penelitian. Tahap akhir dari penelitian ini adalah penulisan laporan penelitian. Laporan penelitian merupakan hasil akhir dari proses penelitian yang disusun secara sistematis dan terstruktur. Laporan penelitian harus memuat semua informasi yang relevan, mulai dari latar belakang penelitian, rumusan masalah, metode penelitian, analisis data, hingga kesimpulan dan saran. Dengan mengikuti tahapan-tahapan tersebut, penelitian ini diharapkan dapat menghasilkan laporan penelitian yang komprehensif, akurat, dan relevan dengan topik yang diteliti.

HASIL DAN PEMBAHASAN

Blockchain adalah teknologi distribusi ledger yang memungkinkan transparansi, keamanan, dan ketahanan data yang tinggi (Shadani & Nasution, 2024). Setiap transaksi yang terjadi akan dicatat dalam sebuah blok, dan blok-blok ini kemudian dihubungkan menjadi rantai yang sangat kuat. Setiap blok memiliki semacam sidik jari unik (*hash*) yang terhubung dengan blok sebelumnya. Jika ada yang mencoba mengubah data dalam salah satu blok, maka semua *hash* setelahnya juga akan berubah, sehingga perubahan tersebut akan langsung terdeteksi. Hal ini membuat data dalam sangat *blockchain* sulit untuk diubah atau diretas (Ghea, 2023).

Blockchain merupakan basis data terdistribusi yang digunakan untuk memelihara daftar record yang terus berkembang, yang disebut dengan blok. Setiap blok mengandung penanda waktu (*timestamp*) dan tautan (*link*) ke blok sebelumnya. Pada umumnya, Blockchain dikelola oleh jaringan *peer-to-peer* yang secara kolektif mematuhi protokol tertentu untuk memvalidasi blok baru (Arief & Sundara, 2017). *Blockchain* secara sederhana, adalah ledger digital terdesentralisasi yang menyimpan catatan transaksi secara permanen dalam bentuk blok yang terhubung dan dienkripsi (E. P. T. Putra & Sutabri, 2024).

Blockchain pertama kali dikembangkan untuk menjawab kebutuhan akan sistem yang lebih efisien, hemat biaya, dan aman dalam mencatat transaksi keuangan di masa depan. Konsep awal *blockchain* muncul pada tahun 1991 saat Stuart Haber dan W. Scott Stornetta menerbitkan artikel berjudul "*How to Time Stamp a Digital Document*" dalam *Journal of Cryptography*. Meskipun pertama kali diterapkan secara nyata pada Bitcoin pada 2009 oleh sosok bernama Satoshi Nakamoto, konsep *blockchain* sebenarnya lebih luas dari sekadar *cryptocurrency*. Bitcoin, sebagai *cryptocurrency*, memanfaatkan jaringan *peer-to-peer* yang terdesentralisasi untuk melakukan verifikasi, persetujuan, dan pemrosesan transaksi tanpa memerlukan perantara, sehingga menjadikannya sistem yang independen (Hasan et al., 2024). Bitcoin adalah sistem pembayaran dan mata uang digital yang dibangun di atas jaringan konsensus terdesentralisasi, yang sepenuhnya dikendalikan oleh para penggunanya. Sementara itu, *blockchain* adalah teknologi di balik Bitcoin dan transaksi lainnya, yang memungkinkan keamanan data dan efisiensi proses dalam berbagai sektor, tidak hanya dalam perdagangan *cryptocurrency* (Ikrima & Darmawan, 2023).

Analisis Teknologi Blockchain Berperan dalam Meningkatkan Keamanan dan Data Privasi di Sektor Keuangan Terhadap Implementasi

Terdapat banyak keterbatasan dalam menjadikan seluruh proses diskresi berbasis *web*, terutama disebabkan oleh kesenjangan digital yang ada. Namun, masalah yang paling mendasar

adalah isu keamanan dan kerahasiaan. Dengan menggunakan *blockchain*, seseorang yang terdaftar dalam daftar pemilih dapat memverifikasi bahwa suaranya telah berhasil dikirimkan sambil tetap anonim. Pada tahun 2014, Liberal Alliance, sebuah partai politik di Denmark, menjadi organisasi pertama yang menggunakan *blockchain* untuk pemungutan suara (Mir, 2017). Dengan tingkat partisipasi pemilih di India yang masih tergolong rendah, pemungutan suara digital yang terdistribusi dapat menjadi solusi untuk memberdayakan mereka yang tidak terdaftar. Meskipun banyak aplikasi *blockchain* saat ini masih dalam tahap pengembangan, potensi masa depan dari aplikasi-aplikasi ini masih terus dieksplorasi. Beberapa tahun ke depan akan difokuskan pada pengujian dan penerapan teknologi ini di berbagai aspek masyarakat. Intinya, *blockchain* memiliki daya tahan yang kuat dan sedang mengubah cara fungsi masyarakat kita. Dengan memanfaatkan teknologi ini, kita tidak hanya dapat meningkatkan keamanan dan kerahasiaan dalam proses pemungutan suara, tetapi juga mendorong partisipasi yang lebih besar dari masyarakat, terutama bagi mereka yang selama ini terpinggirkan dari proses demokrasi. Adopsi yang lebih luas dari sistem voting berbasis *blockchain* diharapkan dapat membawa perubahan signifikan dalam cara kita menjalankan pemilihan umum di masa mendatang.

Blockchain Technology: Challenges And Future Prospects

Di Indonesia sendiri, tidak banyak organisasi yang berani melakukan implementasi teknologi ini ke organisasi mereka dan pengembanagan teknologi ini juga sedikit di wilayah indonesia. Dengan teknologi *Blockchain* orang-orang atau organisasi sangat terbantu dalam hal pengolahan data dari sebuah instansi negara, bidang ekonomi atau pengolahan data lain yang melibatkan suatu organisasi maupun instansi milik negara maka keamanan pada setiap sumber daya data organisasi tersebut harus diperhitungkan. Menggunakan *blockchain* dan kriptografi merupakan upaya menjaga keamanan data organisasi, dimana kriptografi dapat menjaga keamanan pesan dan pesan tersebut tidak dapat di lihat oleh pihak asing. teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi menjadi inti dari mempelajari kriptografi (A. Putra, 2023).

Ada dua jenis algoritma kriptografi berdasar jenis kuncinya (A. Putra, 2023), yaitu:

1. Algoritma Simetri
   Penyebutan lainnya berupa algoritma konvensional, algoritma ini menggunakan kunci enkripsi dan kunci dekripsinya yang sama. Algoritma simetrik nama lainnya yaitu algoritma kunci rahasia, algoritma satu kunci ataupun algoritma kunci tunggal.
2. Algoritma Asimetri
   Kunci enkripsi dan kunci dekripsinya di algoritma ini berbeda, Kunci untuk enkripsi tidak rahasia yang dinamakan kunci publik (*public key*), sedangkan kunci untuk dekripsi rahasia dan namanya yaitu kunci privat (*private key*).

Teknologi *Blockchain* menggambarkan pertumbuhan yang cepat dalam segi popularitas dan kebutuhannya yang ada. Teknologi *blockchain* juga untuk aplikasi yang banyak dan baik, dimana bisa memfasilitasi penggunaannya dalam memberikan solusi yang lebih baik dalam pendekatan tradisional di dunia teknologi. Teknologi *blockchain* dapat mengurangi atau menghindari pemalsuan dokumen resmi. Data *blockchain* dilindungi beberapa lapis teknologi sekunder yaitu *hash*, *hashchain*, *private-public key*, dan distribusi data P2P. Sehingga *blockchain* ideal untuk penyimpanan data publik yang rentan terhadap adanya manipulasi, misalnya seperti pada data identitas penduduk (A. Putra, 2023).

Teknologi utama dalam membangun *blockchain* yaitu berupa *asymmetric key encryption*. Teknik enkripsi yang digunakan pada teknologi blockchain adalah *asymmetric key encryption* atau disebut juga sebagai *public- private key cryptosystem*, dimana setiap *user* atau pengguna membuat dua buah *key* berupa *public key* dan *private key* (teknologi blockchain) dan ada juga keterlibatan fungsi *hash*, *hashchain*, serta *peer-to-peer network*. *Hashing* ini untuk mengubah input menjadi output yang merupakan susunan karakter acak dengan panjang yang telah

ditentukan, dan ini ditentukan sebagai karakter yang unik terhadap masing-masing data yang telah di proses. Contoh fungsi *hash* yaitu *modulo* (A. Putra, 2023).

Hash adalah alat verifikasi untuk memastikan keaslian data dan memastikan blok sebelumnya tidak diubah oleh pihak lain yang tidak berwenang. Dalam *blockchain*, proses input bekerja dengan menambahkan blok baru, sedangkan output-nya berupa rantai yang bekerja dengan menghubungkan blok baru dan blok lama dalam suatu urutan yang tidak bisa diubah, dihapus, atau dibalik. Hal ini dapat diibaratkan seperti jalan satu arah (Nabilla, 2023).

Proses enkripsi ini dapat dienkripsi dan didekripsi, *blockchain* hanya memiliki satu arah, yaitu dari blok baru ke blok lama, sehingga tidak bisa dilakukan modifikasi pada data yang tercatat. Secara singkat, enkripsi ini digunakan untuk mengubah data menjadi *hash*. Setiap transaksi yang masuk ke dalam jaringan *blockchain* akan dienkripsi menjadi *hash*, sehingga tidak dapat diubah atau dihapus (Nabilla, 2023). Begitu suatu data baru telah dimasukkan, maka sistem telah dirancang sedemikian rupa sehingga data tersebut tidak akan pernah dapat dihapus (Putri, 2022).

Dalam memproseskan fungsi teknologi *blockchain*, terdapat konsensus yang memiliki kaitan lewat beberapa node terhubung di dalam jaringan *blockchain* untuk mengkonfirmasi masuknya transaksi. Dengan node-node ini, maka akan dilakukan validasi transaksi dengan membandingkan *hash* yang terkandung di dalamnya dengan *hash* transaksi sebelumnya yang tersimpan pada jaringan. Jika transaksi tersebut valid, maka node-node tersebut akan memberikan konsensus untuk menambahkannya ke dalam jaringan (Nabilla, 2023). Hash terbentuk dari waktu, data yang ada pada *block* dan *hash* sebelumnya. Untuk mendapatkan *hash* pada suatu *block*, diperlukan sumber daya mandiri dari setiap node komputer yang dikelola oleh individu.

Dalam teknologi *blockchain*, terdapat juga mekanisme *proof of work* (PoW) untuk mengatur proses penambahan blok baru ke dalam jaringan, dan merupakan proses yang memerlukan komputer untuk menyelesaikan sebuah *puzzle* matematis yang rumit. Mekanisme PoW membantu menjaga integritas jaringan dengan mencegah terjadinya *spam* atau serangan terhadap jaringan (Nabilla, 2023).

Berdasarkan studi literatur yang ada, teknologi *blockchain* memiliki potensi yang sangat besar dalam meningkatkan keamanan data dan transaksi digital. Beberapa temuan penting dari penelitian ini antara lain:

1. Desentralisasi dan Transparansi: *Blockchain* adalah teknologi transformatif dengan potensi besar untuk merevolusi berbagai industri. Keunggulan utamanya terletak pada desentralisasi dan transparansi, di mana ia beroperasi pada jaringan komputer terdistribusi yang tidak dimiliki oleh satu entitas tunggal. Setiap peserta dalam jaringan memiliki salinan lengkap dari *blockchain*, dan perubahan harus diverifikasi oleh mayoritas jaringan. Hal ini menghilangkan risiko kontrol oleh otoritas pusat dan meningkatkan akuntabilitas karena semua transaksi tercatat secara terbuka dan dapat diaudit oleh siapa saja.
2. Immutabilitas: Salah satu karakteristik terpenting *blockchain* adalah immutabilitasnya. Begitu data dicatat dalam blok dan ditambahkan ke *blockchain*, sangat sulit untuk diubah atau dihapus. Ini karena setiap blok terhubung dengan blok sebelumnya melalui fungsi kriptografi yang kompleks. Sifat ini memastikan integritas data dan membangun kepercayaan dalam sistem.
3. *Smart Contracts*: *blockchain* memfasilitasi penggunaan *smart contracts*, program komputer yang berjalan sendiri yang tersimpan di blockchain. *Smart contracts* dapat secara otomatis mengeksekusi dan menegakkan persyaratan kontrak yang telah disepakati sebelumnya, meningkatkan otomatisasi, kepercayaan, keamanan, dan efisiensi biaya dalam proses bisnis.
4. Penerapan di Berbagai Sektor: Potensi *blockchain* telah terlihat di berbagai sektor. Di industri keuangan, ia memfasilitasi pembayaran dan transfer uang yang lebih cepat, murah,

dan aman. Di bidang logistik dan rantai pasokan, *blockchain* memungkinkan pelacakan pergerakan barang secara *real-time* dan memverifikasi keaslian produk. Dalam bidang kesehatan, *blockchain* dapat menyimpan dan berbagi data medis pasien dengan aman.

Perkembangan pesat teknologi digital telah memudahkan akses, distribusi dan penyimpanan data. Namun, hal ini juga membuka celah bagi beragam ancaman keamanan data yang semakin kompleks. Keamanan data menjadi krusial karena data adalah aset berharga yang dapat memengaruhi keputusan bisnis, menciptakan nilai tambah, dan memberikan keunggulan kompetitif. Oleh karena itu, keamanan data harus menjadi prioritas utama dalam setiap tahap transformasi digital.

Transformasi digital telah membawa perubahan signifikan dalam cara kita berinteraksi, bekerja, dan melakukan bisnis. Data menjadi jantung dari transformasi digital ini, namun juga menjadi target utama serangan siber. Untuk menghadapi tantangan ini, diperlukan pendekatan yang komprehensif dalam menjaga keamanan data. Salah satu teknologi yang menjanjikan dalam meningkatkan keamanan data adalah *blockchain*. Teknologi ini menawarkan tingkat keamanan yang tinggi melalui mekanisme desentralisasi dan kriptografi. Dengan menggunakan *blockchain*, data dapat disimpan secara aman dan transparan, sehingga sulit untuk dimanipulasi atau diubah.

Konsep keamanan data yang mencakup kerahasiaan, integritas, dan ketersediaan menjadi semakin relevan dalam konteks transformasi digital. Kerahasiaan data melindungi informasi pribadi dan bisnis dari penyalahgunaan. Integritas data memastikan data tetap akurat dan dapat dipercaya. Ketersediaan data menjamin kelancaran proses bisnis yang bergantung pada data (Wira Tito, 2023).

Konsep Keamanan Data dalam Transformasi Digital

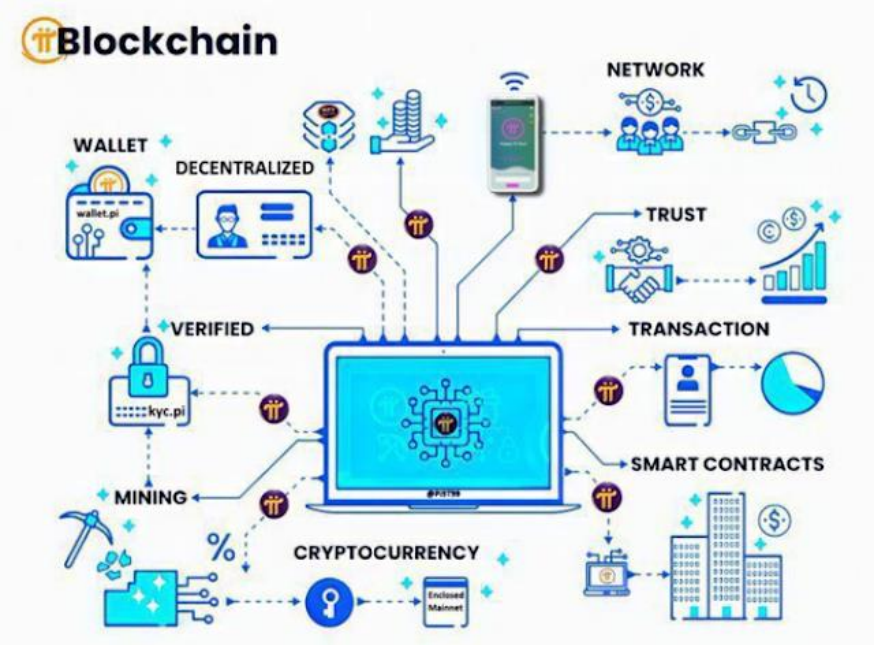
Dalam era digital yang serba cepat, data telah menjadi aset paling berharga bagi organisasi dan individu. Data tidak hanya digunakan untuk membuat keputusan bisnis yang lebih baik, tetapi juga untuk menciptakan produk dan layanan yang inovatif. Namun, seiring dengan meningkatnya ketergantungan pada teknologi digital, risiko keamanan data juga semakin kompleks dan beragam. Serangan siber yang semakin canggih, seperti *ransomware* dan *phishing*, telah menjadi ancaman nyata bagi organisasi di seluruh dunia. Kasus kebocoran data besar-besaran yang terjadi beberapa tahun terakhir menunjukkan betapa pentingnya keamanan data dalam menjaga kepercayaan pelanggan dan melindungi reputasi perusahaan (Cheng et al., 2017). Perkembangan digitalisasi dan penggunaan data pribadi membawa risiko penyalahgunaan data yang semakin tinggi. Kasus kebocoran data, pencurian identitas, dan penyalahgunaan informasi pribadi semakin marak terjadi (Kurnianingrum, 2023).

Konsep keamanan data terdiri dari tiga pilar utama: kerahasiaan, integritas, dan ketersediaan. Kerahasiaan memastikan bahwa data sensitif hanya dapat diakses oleh pihak yang berwenang. Misalnya, data rekam medis pasien harus dijaga kerahasiaannya untuk melindungi privasi pasien. *Blockchain* menjamin integritas data dengan memvalidasi setiap transaksi baru sebelum ditambahkan ke jaringan, sehingga mencegah manipulasi data (Zein, 2024). Integritas menjamin bahwa data tidak diubah atau dirusak oleh pihak yang tidak bertanggung jawab. Keutuhan data memastikan bahwa data lengkap dan akurat. Ketersediaan data menjamin bahwa data dapat diakses kapan pun dibutuhkan untuk mendukung operasi bisnis (Blessing, 2024). Data transaksi tersimpan secara terdesentralisasi dan dapat diakses oleh semua pihak yang terlibat, sehingga mengurangi kebutuhan rekonsiliasi dan meningkatkan transparansi. (penerapan) Ancaman terhadap keamanan data dapat berasal dari berbagai sumber, baik internal maupun eksternal. Serangan siber seperti *ransomware*, *phishing*, dan serangan *DDoS* (*Distributed Denial of Service*) merupakan ancaman yang semakin umum dan berbahaya. Serangan ini dapat menyebabkan hilangnya data, gangguan operasional, dan kerugian finansial yang besar. Kesalahan manusia, seperti mengklik tautan *phishing* atau meninggalkan perangkat yang tidak terkunci, dapat membuka pintu bagi penyerang untuk

mengakses data sensitif. Kegagalan perangkat keras atau lunak dapat menyebabkan hilangnya data atau gangguan operasional. Kebocoran data dapat terjadi akibat kesalahan konfigurasi sistem, serangan siber, atau kesalahan manusia.

Untuk melindungi data dari ancaman yang ada, organisasi perlu menerapkan strategi keamanan data yang komprehensif. Langkah-langkah yang dapat diambil meliputi implementasi kontrol akses, enkripsi data, pencadangan data, pembaruan perangkat lunak, pelatihan kesadaran keamanan, pemantauan dan analisis, serta pengujian penetrasi. Keamanan data merupakan hal yang sangat penting di era digital saat ini. Dengan menerapkan strategi keamanan yang komprehensif, organisasi dapat melindungi data sensitif mereka dari ancaman yang ada. Penting untuk diingat bahwa keamanan data merupakan proses yang berkelanjutan, dan organisasi harus terus beradaptasi dengan ancaman baru yang muncul. Teknologi Blockchain telah muncul sebagai solusi menarik untuk mengatasi tantangan keamanan data utama, namun, beberapa *platform blockchain* masih menghadapi kendala dalam meningkatkan kapasitas dan kinerja jaringan untuk menangani beban kerja yang berat (Sinulingga & Nasution, 2024).

Untuk membangun pertahanan yang kuat terhadap ancaman siber, organisasi perlu mengadopsi pendekatan keamanan yang komprehensif. Selain teknologi keamanan, peran manusia sangat penting dalam menjaga keamanan data. Pelatihan kesadaran keamanan siber bagi karyawan harus menjadi bagian integral dari program keamanan data. Selain itu, organisasi juga perlu melakukan penilaian risiko secara berkala untuk mengidentifikasi kelemahan dalam sistem keamanan mereka dan mengambil tindakan perbaikan yang diperlukan.



Gambar 1. *Future of Digital Transaction with Blockchain*

Blockchain adalah sistem terdesentralisasi yang memungkinkan transaksi aman dan transparan tanpa pihak ketiga. Dalam diagram ini, *wallet, decentralized, verified,* dan *mining* adalah beberapa komponen penting yang bekerja bersama untuk memfasilitasi transaksi. *Wallet* bertindak sebagai wadah digital untuk menyimpan *cryptocurrency*. *Decentralized* berarti bahwa *blockchain* tidak dikendalikan oleh satu entitas tunggal, memastikan transparansi dan keamanan. *Verified* mengacu pada proses verifikasi identitas dan transaksi yang dilakukan melalui *blockchain*. *Mining* adalah proses yang digunakan untuk memvalidasi dan

menambahkan transaksi baru ke *blockchain*. Pada saat transaksi dilakukan, setiap pengguna akan mencatat dan menyimpan sebagai data baru (Sugandi et al., 2022). Setelah transaksi divalidasi, mereka dicatat dalam *blockchain*, yang merupakan catatan digital yang tidak dapat diubah yang disimpan di seluruh jaringan. *Cryptocurrency*, yang disimpan dalam *wallet*, dihubungkan ke jaringan melalui *mainnet*. Jaringan ini, melalui *trust* dan *transaction*, menggunakan *Smart Contract* untuk memfasilitasi berbagai aplikasi *blockchain*, seperti membangun aplikasi terdesentralisasi.

Blockchain juga menawarkan privasi yang tinggi selain keamanan utamanya, untuk itu terdapatlah sistem atau teknologi yang bertugas menjamin anonimitas pengguna dan privasi data yang tersimpan di dalamnya (Nabilla, 2023), yaitu:

1. Sistem Pseudonim
   Sistem Pseudonim: Sistem ini digunakan untuk menyimpan identitas pengguna dalam jaringan blockchain. Pengguna hanya perlu menggunakan alamat unik (*public key*) untuk menerima dan mengirim transaksi. Dengan begitu, maka transaksi yang ada dalam jaringan *blockchain* tidak dapat dilacak kembali ke individu yang bersangkutan. Sistem pseudonim ini membantu menjaga privasi pengguna dan mencegah terjadinya pelacakan transaksi.
2. Teknologi *Zero Knowledge Proof (Zk-SNARK)*
   Teknologi ini digunakan dalam membuktikan kebenaran suatu informasi tanpa perlu mengekspos informasi tersebut ke pihak lain. Secara singkat, *zk-SNARK* ini untuk meningkatkan tingkat anonimitas pengguna dan privasi data dalam jaringan blockchain.
3. Teknologi *Mixnet*
   Teknologi ini digunakan untuk mencampurkan transaksi dari berbagai pengguna sehingga mustahil dilacak kembali oleh individu yang bersangkutan. Teknologi ini menggunakan node yang tersebar di seluruh jaringan, gunanya untuk mencampurkan transaksi yang masuk sehingga tidak dapat dilacak kembali. Maka dengan itu, *mixnet* mampu meningkatkan privasi transaksi dalam jaringan *blockchain*.

Dengan adanya teknologi-teknologi ini, pengguna *blockchain* dapat bertransaksi dengan aman dan menjaga privasi mereka. Teknologi *blockchain* terus berkembang dan akan semakin canggih di masa depan. Penerapan teknologi *blockchain* pada organisasi akan membantu pengolahan data yang ada pada organisasi menjadi efektif, efisien, aman dan transparan. (1274) Dengan demikian, diharapkan dapat menciptakan ekosistem digital yang lebih aman dan terjamin privasi penggunanya.

Saat ini, *blockchain* berada di tahap penting yang memerlukan transisi dari bukti konsep ke implementasi nyata. Proses ini memerlukan kerjasama antara semua pihak yang terlibat. Seperti mobil yang tidak dapat digunakan tanpa jalan, *blockchain* hanya akan berharga sejauh infrastruktur yang ada untuk mendukungnya. Banyak aplikasi potensial dari teknologi *blockchain* memerlukan keterlibatan pemerintah agar dapat berjalan dengan efektif. Misalnya, dalam situasi di mana sertifikat kepemilikan (sertifikat kepemilikan) harus didigitalisasi agar skenario tersebut berfungsi (Hreinsson & Blöndal, 2018).

Di sisi efisiensi, *blockchain* diyakini dapat mengubah cara perusahaan mengelola operasional dan strateginya. Teknologi ini menyediakan opsi tak terbatas, tetapi penerapannya yang berhasil akan sangat bergantung pada strategi fokus dan selektif. Sebagai contoh, manajemen perusahaan dapat memilih antara mengembangkan teknologi *blockchain* secara internal, yang menawarkan fleksibilitas namun memerlukan biaya pengembangan dan pemeliharaan yang tinggi, atau memilih *Blockchain as a Service* (BaaS). Pilihan BaaS menawarkan penghematan biaya sekaligus meningkatkan performa operasional perusahaan tanpa terbebani oleh kompleksitas teknologi. Model ini diharapkan dapat meningkatkan efisiensi bisnis, sehingga menghasilkan layanan baru dan meningkatkan efisiensi operasional tanpa risiko biaya tinggi. Teknologi *blockchain* mendasari mata uang digital Bitcoin. Ini adalah domain terdesentralisasi untuk transaksi, di mana setiap transaksi dicatat dalam buku besar

publik yang dapat diakses oleh semua orang. Tujuan dari *blockchain* adalah untuk memberikan kerahasiaan, keamanan, perlindungan, dan transparansi bagi semua penggunanya. Namun, karakteristik ini juga menimbulkan berbagai tanta ngan teknis dan keterbatasan yang perlu diatasi (Levis et al., 2021).

Blockchain memungkinkan pengembangan sistem baru yang lebih berbasis pada keputusan partisipatif dan organisasi terdesentralisasi, yang dapat beroperasi di jaringan komputer tanpa intervensi manusia. Banyak orang membandingkan *blockchain* dengan internet, dengan harapan bahwa teknologi ini akan mengubah keseimbangan kekuasaan dari pihak-pihak yang terpusat dalam bidang komunikasi dan bisnis. Dengan penerapan teknologi ini, semua transaksi perbankan dapat menjadi lebih cepat dan murah, sehingga penghematan tersebut dapat dialokasikan untuk kesejahteraan sosial atau keamanan digital (Levis et al., 2021).

Seperti semua teknologi baru, dampak jangka panjangnya akan terlihat seiring waktu. Keberhasilan suatu inovasi teknologi sangat tergantung pada kemampuannya untuk menciptakan nilai. Salah satu keuntungan yang tidak diragukan dari teknologi *blockchain* adalah kemampuannya untuk mengatasi masalah kepercayaan saat mentransfer nilai. (journal.pone) Masa depan *blockchain* akan bergantung pada kemampuannya untuk memberikan efisiensi dan penghematan biaya bagi penggunanya. Jika *blockchain* berhasil menciptakan nilai dan meningkatkan kesejahteraan sosial, maka adopsi pengguna dan investasi tambahan akan mengikuti. Wajar untuk tidak mengharapkan bahwa setiap implementasi *blockchain* akan sempurna di tahap awal. Banyak tantangan yang masih perlu diatasi sebelum teknologi ini dapat mencapai potensi penuhnya. Proses ini akan membutuhkan kolaborasi antara semua pemangku kepentingan terkait, dan kemungkinan besar akan memakan waktu. Adopsi teknologi *blockchain* dapat menjadi ancaman bagi bisnis dalam industri layanan keuangan. Oleh karena itu, tidak realistis untuk beranggapan bahwa akan ada ketidakberdayaan dari mereka yang mendapat keuntungan dari sistem yang ada. Industri layanan keuangan telah menunjukkan kekuatan lobi yang signifikan dalam politik global. Kesimpulan dari analisis ini adalah bahwa kita berada di ambang revolusi teknologi baru—revolusi *blockchain*. Proses ini mungkin akan memakan waktu dan diwarnai oleh tantangan, tetapi dampaknya kelak bisa sebanding dengan pengaruh internet (Hreinsson & Blöndal, 2018).

Manfaat dan Risiko Penggunaan *Blockchain* untuk Keamanan Data

Penggunaan teknologi *blockchain* dalam meningkatkan keamanan data telah menjadi sorotan utama dalam beberapa tahun terakhir. Tidak seperti sistem penyimpanan data konvensional yang terpusat dan rentan terhadap serangan, *blockchain* menawarkan pendekatan yang lebih aman dan transparan. Dalam *blockchain*, data disimpan dalam blok-blok yang saling terhubung dan terenkripsi secara kuat. Setiap transaksi atau data yang ditambahkan ke dalam *blockchain* akan diverifikasi oleh seluruh jaringan, sehingga sangat sulit untuk dimanipulasi atau dihapus. Hal ini memberikan tingkat keamanan yang jauh lebih tinggi dibandingkan dengan *database* tradisional (Wira Tito, 2023).

Selain keamanan yang tinggi, *blockchain* juga menawarkan transparansi yang tak tertandingi. Setiap transaksi dan data yang tercatat dalam *blockchain* dapat dilacak dan diverifikasi oleh siapa saja. Misalnya, dalam industri farmasi, *blockchain* dapat digunakan untuk melacak perjalanan suatu obat dari produsen hingga konsumen, sehingga dapat mencegah pemalsuan obat dan memastikan kualitas produk. Transparansi ini tidak hanya meningkatkan kepercayaan konsumen, tetapi juga dapat meningkatkan efisiensi rantai pasok (Wira Tito, 2023).

Pemerintah Indonesia juga melakukan kerja sama dengan beberapa perusahaan *blockchain*, yang tentunya untuk peningkatan solusi keamanan data. Dengan menggunakan teknologi *blockchain*, proses verifikasi dan validasi sertifikat atau dokumen penting dapat dilakukan dengan cepat dan efisien. Infrastruktur digital yang cepat dan stabil diperlukan dalam

mengadopsi teknologi *blockchain*, karena teknologi *blockchain* memerlukan akses internet yang cepat dan stabil. Kurangnya infrastruktur yang menjadi salah satu penghambat di indonesia, dimana digital yang tidak memadai dapat mempersulit implementasi teknologi *blockchain*. Sehingga keamanan dengan menggunakan teknologi *blockchain* menjadi tertunda atau terhambat untuk melaksanakan tugasnya (Politou et al., 2019).

Meskipun ada kekhawatiran tentang keamanan, privasi, dan regulasi teknologi *blockchain*, potensi aplikasi *blockchain* di berbagai bidang, seperti seni, pariwisata, dan olahraga, sangat menjanjikan. Di dunia seni, *blockchain* memungkinkan perlindungan hak cipta yang lebih kuat, pelacakan kepemilikan karya seni yang transparan, dan cara baru bagi seniman untuk memonetisasi karya mereka melalui NFT. NFT mengubah karya seni digital menjadi aset unik dan bernilai yang dapat diperdagangkan secara aman di pasar global.

Di sektor pariwisata, *blockchain* mempermudah transaksi yang lebih cepat, aman, dan transparan bagi wisatawan dan operator tur. Mata uang digital atau kripto memungkinkan wisatawan melakukan pembayaran internasional tanpa konversi mata uang yang rumit atau biaya transfer antar bank. *Blockchain* juga dapat digunakan untuk menyimpan dan memverifikasi identitas digital pelancong, yang mempercepat proses imigrasi dan meningkatkan keamanan data pribadi. Di dunia olahraga, *blockchain* berpotensi merevolusi manajemen tiket, hak siar, dan hubungan antara penggemar dan atlet. Penggemar dapat mengakses tiket digital yang aman, mengurangi pemalsuan tiket dan percaloan. *Blockchain* juga memungkinkan penggemar untuk mendukung atlet atau tim favorit mereka secara langsung melalui *crowdfunding* berbasis *blockchain* yang transparan.

Meskipun masih dalam tahap awal, potensi ekonomi *blockchain* tidak dapat diabaikan. Adopsi yang lebih luas akan mendorong inovasi dan efisiensi di berbagai sektor, membantu organisasi mengatasi tantangan yang sulit dipecahkan. *Blockchain* meningkatkan transparansi dan kecepatan transaksi, serta memberikan solusi yang lebih aman untuk pengelolaan data dan informasi sensitif. Adopsi *blockchain* yang lebih luas di masa depan diharapkan memberikan dampak positif yang signifikan bagi ekonomi global, meningkatkan produktivitas, dan membuka peluang baru. Dengan perencanaan dan regulasi yang tepat, *blockchain* dapat menjadi dasar bagi ekosistem digital yang lebih aman, transparan, dan efisien, membawa kemajuan di berbagai bidang kehidupan manusia.

Analisis terhadap temuan penelitian mengindikasikan bahwa teknologi *blockchain* memiliki potensi transformatif yang signifikan, khususnya dalam meningkatkan keamanan data dan transaksi pada berbagai sektor.

1. Kepercayaan yang Terbangun
    a. Transparansi Tak Terbantahkan: Setiap transaksi yang dilakukan di *blockchain* dicatat secara publik dan permanen dalam buku besar yang terdesentralisasi. Hal ini memungkinkan siapa pun untuk memverifikasi setiap transaksi, memastikan transparansi dan akuntabilitas yang tinggi.
    b. Sifat Immutabilitas: Setelah sebuah transaksi dicatat dalam *blockchain*, data tersebut tidak dapat diubah atau dihapus. Sifat immutabilitas ini menjamin keautentikan dan integritas data, menghilangkan risiko manipulasi atau pemalsuan.
    c. Mekanisme Konsensus: *Blockchain* menggunakan mekanisme konsensus yang kuat untuk memvalidasi setiap transaksi. Dalam proses ini, node-node dalam jaringan bekerja sama untuk mencapai kesepakatan tentang validitas transaksi sebelum menambahkannya ke dalam *blockchain*. Mekanisme ini memastikan bahwa hanya transaksi yang sah yang dapat ditambahkan ke dalam sistem.
2. Efisiensi dan Otomatisasi
    a. *Smart Contracts*: *Smart Contracts* adalah program komputer yang berjalan secara otomatis di *blockchain*. Mereka memungkinkan pelaksanaan perjanjian secara digital,

tanpa memerlukan perantara atau campur tangan manusia. Hal ini mempercepat waktu penyelesaian transaksi, mengurangi biaya, dan meningkatkan efisiensi.

b. Pengurangan Biaya: Dengan menghilangkan perantara seperti bank atau lembaga keuangan lainnya, *blockchain* dapat mengurangi biaya transaksi secara signifikan. Hal ini terutama bermanfaat dalam sektor keuangan, di mana biaya transaksi tradisional bisa sangat tinggi

3. Keamanan yang Tingkat Tinggi
   a. Desentralisasi: *Blockchain* adalah jaringan terdesentralisasi, yang berarti data tidak disimpan di satu lokasi pusat. Hal ini membuatnya lebih tahan terhadap serangan dibandingkan sistem terpusat, yang rentan terhadap serangan tunggal.
   b. Kriptografi yang Kuat: *Blockchain* menggunakan algoritma kriptografi yang canggih untuk melindungi data pengguna dari akses yang tidak sah. Enkripsi yang kuat memastikan bahwa hanya pihak yang berwenang yang dapat mengakses informasi sensitif.
4. Potensi Penerapan yang Luas
   a. Sektor Keuangan: *Blockchain* dapat merevolusi sistem pembayaran, memungkinkan transaksi yang lebih cepat, murah, dan aman. Teknologi ini juga dapat digunakan untuk manajemen aset, penerbitan saham, dan layanan keuangan lainnya.
   b. *Supply Chain*: *Blockchain* dapat meningkatkan transparansi dan efisiensi dalam rantai pasok. Dengan mencatat setiap langkah dalam proses, *blockchain* memungkinkan pelacakan produk dari asal hingga tujuan, mengurangi risiko pemalsuan dan meningkatkan kepercayaan konsumen.
   c. Pemerintahan: *Blockchain* dapat digunakan untuk menciptakan sistem pemungutan suara yang lebih aman dan transparan. Teknologi ini juga dapat digunakan untuk mengelola catatan publik, seperti sertifikat kelahiran, pernikahan, dan kematian.

Selain dengan begitu banyak keunggulan yang di dapatkan dari teknologi *blockchain*, teknologi ini juga memiliki keterbatasan dan tantangan tersendiri. Misalnya, skalabilitas dan biaya transaksi masih menjadi kendala bagi beberapa aplikasi, juga ada beberapa keterbatasan seperti data yang tidak *portable*, tidak ada regulasi dan standar, serta keamanan dari *private key*-nya. Meskipun sistem blockchain sulit dimanipulasi, tetapi masih mungkin dalam melakukan serangan 51% jika mayoritas kekuatan komputasi di jaringan dikendalikan satu entitas (A. Putra, 2023).

Tantangan atau risiko keamanan dalam sistem blockchain yang perlu dipahami:

1. Serangan 51% (51% *attacks*), merupakan ancaman serius bagi jaringan *blockchain*. Penyerang yang mengendalikan lebih dari 50% kekuatan komputasi jaringan dapat melakukan beberapa hal yang merugikan pengguna. Seperti membatalkan transaksi yang sudah dilakukan dan mengembalikan dana ke pengirim, penyerang juga dapat menambah blok baru ke *blockchain* yang berisi transaksi palsu, aturan konsensus jaringan seperti mekanisme penambangan atau proses validasi transaksi juga dapat diubah oleh penyerang 51% ini (Alia & S ST, 2024).
2. Kerentanan *smart contract,* kesalahan dalam logika kode *smart contract* dapat menyebabkan hasil yang tidak diinginkan, seperti kehilangan data atau manipulasi data. Kerentanan keamanan dalam kode *smart contract* dapat dieksploitasi oleh penyerang untuk mencuri dana atau mengendalikan aset.
3. Serangan DdoS, cara kerjanya membajiri jaringan *blockchain* dengan permintaan berlebihan, sehingga menyebabkan gangguan layanan dan membuat transaksi sulit dilakukan, hal ini menyebabkan kerugian finansial bagi pengguna dan pengembang *blockchain*.

4. Pencurian kunci pribadi atau kunci kriptografi yang digunakan untuk mengakses dan mnegontrol aset digital di *blockchain* dengan menggunakan *malware, phising,* atau serangan *social engineering.*
5. Risiko regulasi, regulasi *cryptocurrency* yang berbeda-beda di berbagai negara dapat menciptakan ketidakpastian bagi investor dan pengembang.

Terdapat beberapa cara juga untuk meningkatkan keamanan sistem *blockchain* dan menghindari risiko keamanan yang ada (Nabilla, 2023), yaitu dengan:

1. *Cold Storage*
   Di mana aset disimpan di perangkat keras yang tidak terhubung ke internet seperti *hard drive* atau *flash drive*. Karena tidak terhubung ke internet, aset digital di dalam *cold storage* tidak dapat diakses oleh pihak yang tidak bertanggung jawab.
2. *Multisignature*
   Cara ini mengatur agar setiap transaksi hanya dapat dilakukan jika ada persetujuan dari beberapa pihak. Jadi, semua pihak yang terlibat harus memberikan persetujuan agar transaksi dapat diproses. *Multisignature* sangat efektif untuk meminimalkan risiko penipuan atau pemalsuan.
3. Audit Keamanan
   Berupa cara mengecek dan memperbaiki kelemahan keamanan sistem. Ini dilakukan secara berkala untuk memastikan sistem tidak ada kelemahan yang bisa dimanfaatkan pihak yang tidak bertanggung jawab.
4. Memperkuat keamanan jaringan
   Dengan menggunakan mekanisme konsensus yang lebih canggih dan tahan terhadap serangan, seperti *Proof-of-Stake* (PoS) atau *Proof-of-Authority* (PoA).

KESIMPULAN

Berdasarkan hasil dan pembahasan penelitian, maka dapat ditarik kesimpulan bahwa perkembangan teknologi digital telah membawa perubahan besar dalam cara kita berinteraksi, berbisnis, dan menyimpan data. Namun, kemajuan ini juga memunculkan tantangan baru dalam hal keamanan data dan transaksi, yang semakin kompleks dengan ancaman kejahatan siber yang canggih. Teknologi blockchain muncul sebagai solusi yang menjanjikan, dengan keunggulan desentralisasi, transparansi, dan kriptografi yang kuat. Blockchain menawarkan tingkat keamanan yang tinggi, dimana setiap transaksi diverifikasi oleh seluruh jaringan, memastikan integritas data yang tersimpan. Keunggulan lain dari blockchain adalah sifat immutabilitasnya, yang menjaga keautentikan data dan mengurangi kemungkinan manipulasi.

Selain itu, blockchain juga meningkatkan efisiensi melalui smart contracts, yang memungkinkan otomatisasi proses bisnis dan mengurangi risiko kesalahan manusia. Penghapusan perantara dalam transaksi juga mengurangi biaya. Penerapan blockchain yang luas di sektor keuangan, rantai pasok, pemerintahan, dan kesehatan menunjukkan fleksibilitas teknologi ini dalam memberikan solusi untuk berbagai tantangan. Meskipun demikian, blockchain juga menghadapi tantangan seperti skalabilitas, biaya transaksi, dan masalah keamanan private key. Regulasi yang jelas juga diperlukan untuk mendukung penerapan teknologi ini secara optimal. Dengan kolaborasi dan inovasi yang terus berkembang, blockchain memiliki potensi besar untuk merevolusi cara kita mengamankan data dan transaksi di masa depan, meningkatkan kepercayaan pengguna terhadap integritas sistem.

DAFTAR PUSTAKA

Alia, P. A., & S ST, M. T. (2024). *Keamanan Sistem Informasi*. Penamuda Media.

Arief, L., & Sundara, T. A. (2017). Studi atas pemanfaatan blockchain bagi Internet of Things (IoT). *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *1*(1), 70–75.

Blessing, M. (2024). *Impact on Data Integrity and Privacy*.

Chairunnas, A., Sugianto, E., Pratiwi, R., Sitorus, M., & Cahyono, B. (2024). Teknologi Blockchain dalam Transformasi Keuangan dan Perbankan: Potensi dan Tantangan. *Journal of Economic Education and Entrepreneurship Studies*, *5*(2), 357–368.

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5), e1211.

Damanik, D. F., & Nasution, M. I. P. (2024). Analisis Penggunaan Teknologi Blockchain Dalam Pengelolaan Keamanan Data Pada Big Data. *Jurnal Ilmiah Nusantara*, *1*(4), 718–724.

Dhanu Prayogo, S. H., Shivendra Adistya, S. H., Eliadi Hulu, S. H., & Nikita Johanie, S. H. (2022). *Mengenal Hukum Aset Kripto*. Deepublish.

Djumadi, D. (2024). Teknologi Blockchain dalam Perspektif Ekonomi/Keuangan Islam. *Al-Kharaj: Jurnal Ekonomi, Keuangan & Bisnis Syariah*, *6*(3), 3897–3915.

Hasan, Z., Wiryadi, W., Fadhulrrahman, A., Dimas, M., & Al Jabbar, R. D. (2024). Regulasi Penggunaan Teknologi Blockchain Dan Mata Uang Kripto Sebagai Tantangan Di Masa Depan Dalam Hukum Siber. *Birokrasi: Jurnal Ilmu Hukum Dan Tata Negara*, *2*(2), 55–69.

Hendrayana, I. G., Suprayitno, D., Judijanto, L., Kosadi, F., Kusumastuti, S. Y., & Sepriano, S. (2024). *E-Money: Panduan Lengkap Penggunaan dan Manfaat E-Money dalam Era Digital*. PT. Sonpedia Publishing Indonesia.

Herlina, H., Ningsih, L. A., & Sari, N. (2023). Kehalalan Transaksi Online Shop Dalam Perspektif Hukum Ekonomi Syariah. *Jurnal Ilmiah Mahasiswa Perbankan Syariah (JIMPA)*, *3*(2), 431–444.

Hidayat, M. S., Sujianto, A. E., & Asiyah, B. N. (2023). Mengkaji Sistem Keuangan Berbasis Teknologi Blockchain dalam Ekonomi Moneter Islam. *MUQADDIMAH: Jurnal Ekonomi, Manajemen, Akuntansi Dan Bisnis*, *1*(3), 244–262.

Hildawati, H., Haryani, H., Umar, N., Suprayitno, D., Mukhlis, I. R., Sulistyowati, D. I. D., Budiman, Y. U., Saktisyahputra, S., Faisal, F., & Thomas, A. (2024). *Literasi Digital: Membangun Wawasan Cerdas dalam Era Digital terkini*. PT. Green Pustaka Indonesia.

Hreinsson, E. M., & Blöndal, S. P. (2018). *The future of blockchain technology and cryptocurrencies.*

Ikrima, S. P., & Darmawan, S. (2023). Analisis Volatily Spillover Bitcoin Terhadap Ethereum, Tether, dan Emas Dunia Menggunakan Metode EGARCH. *Jurnal Manajemen Dan Perbankan (JUMPA)*, *10*(2), 47–60.

Kiki Kristanto, S. H., Nurjamil, S. H. I., Jaya, I. K. N. A., Kom, S., & Joanita Jalianery, S. H. (2024). *Transformasi hukum dalam era revolusi teknologi blockchain: buku referensi*. PT. Media Penerbit Indonesia.

Kurnianingrum, T. P. (2023). Urgensi pelindungan data pribadi konsumen di era ekonomi digital. *Kajian*, *25*(3), 197–216.

Levis, D., Fontana, F., & Ughetto, E. (2021). A look into the future of blockchain technology. *Plos One*, *16*(11), e0258995.

Madya, A. D., Haryanto, B. D., Ningsih, D. P., & Sinlae, F. (2023). Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman Cybersecurity. *Indonesian Journal of Education And Computer Science*, *1*(3), 127–135.

Mir, W. A. (2017). Necessity and implementation of blockchain technology. *International Journal of Scientific Research and Management (IJSRM)*, *5*(07), 6279–6280.

Nabilla, G. R. (2023). Tren Keamanan Informasi berbasis Blockchain di Masa Kini dan di Masa Mendatang. *Researchgate.Net*. https://www.researchgate.net/publication/370073770_Tren_Keamanan_Informasi_berbasis_Blockchain_di_Masa_Kini_dan_di_Masa_Mendatang

Nugroho, I. I., Pratiwi, R., & Zahro, S. R. A. (2021). Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, *1*(2), 115–129.

Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing*, *9*(4), 1972–1986.

Putra, A. (2023). Penggunaan Teknologi Blockchain Dalam Upaya Meningkatkan Keamanan Data Di Massa Era Digital. *No. April*, 1–11.

Putra, E. P. T., & Sutabri, T. (2024). Penerapan Teknologi Blockchain dalam Transformasi Model Bisnis di Industri Keuangan Digital. *IJM: Indonesian Journal of Multidisciplinary*, *2*(3), 76–82.

Putri, J. H. (2022). *Perancangan dan implementasi teknologi blockchain pada transaksi wakaf produktif*. Fakultas Sains dan Teknologi UIN Syarif Hidayatullah Jakarta.

Setianingsih, R., & Nasution, M. I. P. (2024). Analisis Teknologi Blockchain Berperan dalam Meningkatkan Keamanan dan Data Privasi di Sektor Keuangan Terhadap Implementasi. *Jurnal Ilmiah Nusantara*, *1*(4), 588–596.

Shadani, D., & Nasution, M. I. P. (2024). Optimalisasi Pengelolaan Informasi Data Untuk Peningkatan Kualitas Layanan Di Era Digital. *Journal Of Informatics And Busisnes*, *2*(1), 47–51.

Sinulingga, C. R., & Nasution, M. I. P. (2024). Analisis Penggunaan Teknologi Blockchain Dalam Pengelolaan Big data. *Jurnal Ilmiah Nusantara*, *1*(4), 530–536.

Sugandi, H. K., Harahap, N. S., Cynthia, E. P., Yanto, F., & Sanjaya, S. (2022). Rancang Bangun Aplikasi Simulasi Mining Pada Jaringan Blockchain Bitcoin. *Sebatik*, *26*(1), 332–339.

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.

Tuna, M. S. (2024). Implementasi Blockchain Dalam Lembaga Keuangan Perbankan. *LEX Administratum*, *12*(5).

Zein, A. (2024). Teknologi Blockchain dan AI Dalam Aplikasi E Commerce. *Marketica: Jurnal Ilmiah Pemasaran*, *1*(4), 172–180.