Jurnal Infotronik Volume 8 No. 2, Desember 2023 P-ISSN: 2548-1932
e-ISSN: 2549-7758

ANALISIS KEAMANAN PADA TEKNOLOGI BLOCKCHAIN

Zen Munawar[1], Novianti Indah Putri[2], Iswanto[3], Dandun Widhiantoro[4]

[1] Manajemen Informatika, Politeknik LP3I
[2] Sistem Informasi, Universitas Kebangsaan Republik Indonesia
[3] Teknik Informatika, Universitas Nurtanio Bandung
[4] Teknik Elektro Informatika, Politeknik Negeri Jakarta
[1] munawarzen@gmail.com

ABSTRACT

Blockchain technology has great potential with a wide range of applications and provides broad opportunities for various infrastructures. Blockchain is a decentralized technology, that having broad power to solve business problems. Blockchain is emerging as a technology that promises to ensure higher levels of data encryption and security. This research aims to analyze security in blockchain technology. Transaction protection can use blockchain Security blocks against internal, malicious, peripheral and accidental threats. Analysis was carried out on the blockchain security framework architecture and as the system security model used in blockchain technology It is necessary to integrate existing security architectures with blockchain-based applications regarding technological and organizational issues. Terminal devices, networks, and super-node servers as part of the infrastructure tier. Security contributions can be mapped according to these three levels. Research discussions also on blockchain technology security architecture, frameworks, and standards and frameworks to reduce cybersecurity risks when using blockchain technology. With this research we hope to improve the current literature on blockchain security and propose future research.

Keywords: *Blockchain Technology, Blockchain Security, Data Security, Security Standards*

ABSTRAK

Teknologi blockchain memiliki potensi besar dengan beragam aplikasi dan memberikan peluang luas untuk berbagai infrastruktur. Blockchain adalah teknologi terdesentralisasi, memiliki kekuatan yang luas untuk memecahkan masalah bisnis. Blockchain muncul sebagai teknologi yang dijanjikan untuk memastikan tingkat enkripsi dan keamanan data yang lebih tinggi. Penelitian ini bertujuan untuk menganalisis keamanan pada teknologi blockchain. Keamanan Blockchain adalah perlindungan transaksi dalam blok terhadap ancaman internal, jahat, periferal, dan tidak disengaja. Analisis dilakukan pada arsitektur kerangka keamanan blockchain serta model keamanan sistem yang digunakan pada teknologi blockchain. Perlu melakukan integrasi arsitektur keamanan yang ada dengan aplikasi berbasis blockchain mengenai masalah teknologi dan organisasi. Level infrastruktur mencakup perangkat terminal, jaringan, dan server super-node. Kontribusi keamanan dapat dipetakan menurut ketiga tingkatan tersebut. Hasil penelitian ini pada arsitektur, kerangka, dan standar keamanan teknologi blockchain dan kerangka kerja untuk mengurangi risiko keamanan dunia maya saat menggunakan teknologi blockchain. Dengan penelitian ini semoga dapat meningkatkan literatur mutakhir tentang keamanan blockchain dan mengusulkan penelitian di masa depan.

Kata Kunci: *Teknologi Blockchain, Keamanan Blockchain, Keamanan Data, Standar Keamanan*

PENDAHULUAN

Blockchain adalah struktur data terdistribusi yang terdiri dari blok rantai, bisa berupa buku besar global yang menyimpan catatan semua transaksi di jaringan blockchain. Dengan adopsi bitcoin yang cepat dan meluas, blockchain dipuji sebagai inovasi dalam paradigma komputasi [1]. Teknologi blockchain memiliki potensi besar dengan beragam aplikasi dan memberikan peluang luas untuk berbagai infrastruktur. Teknologi ini mendorong manajemen sumber daya dan membuat komunikasi menjadi aman dan

efisien. Kepercayaan meningkat saat melakukan transaksi keuangan antar pihak menggunakan blockchain, karena mengurangi kemungkinan penipuan dan secara otomatis menghasilkan catatan aktivitas. Blockchain merupakan paradigma komputasi baru yang aman dan bermanfaat untuk mendukung inovasi bisnis [2].

Direktur perusahaan dengan bantuan intelijen bisnis melakukan analisis dalam mengambil keputusan [3]. Organisasi dengan bantuan big data dapat menganalisis dengan cepat serta akurat pada ukuran data yang besar [4]. Membuat pemeriksaan latar belakang otomatis dari setiap anggota sistem. Karena sifatnya yang terdesentralisasi, blockchain mempunyai sifat terdesentralisasi sehingga mengurangi risiko aktivitas penipuan dan akses tidak sah ke data sensitif.

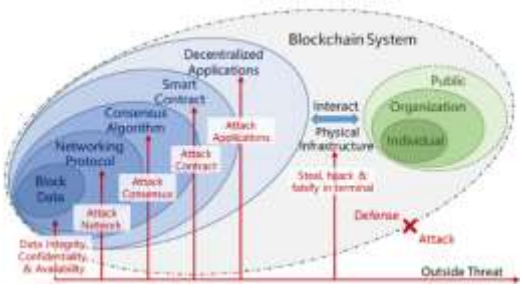
Hasil menunjukkan pendekatan ini memiliki kinerja yang baik [5]. Saat ini semua orang menggunakan teknologi canggih untuk berkomunikasi melalui internet. Panggilan suara, panggilan video, pesan, gambar, dikirim langsung dari pengirim ke penerima melalui internet. Untuk transaksi ini, harus memelihara pihak ketiga yang terpercaya antara pengirim dan penerima ini. Pengawasan diperlukan agar teknologi bisa berjalan sesuai dengan yang diharapkan [6]. Big data mempunyai kemampuan dalam mengelola volume data, kecepatan data, variasi serta kebenaran dari data.[7]. Data mempunyai peran penting karena organisasi bisa berjalan dengan baik dengan adanya data sebagai fondasinya. [8].

Dalam hal transaksi uang, orang harus mempercayai pihak ketiga untuk menyelesaikannya, dalam sistem tradisional. Transaksi bisa dilakukan dengan pemanfaatan QRIS sebagai alat pembayaran [9]. Tetapi dalam kasus blockchain itu akan memberikan keamanan yang sempurna dalam bertransaksi. Sebuah blok harus mencatat setiap transaksi, itu akan bertindak seperti buku catatan. Setelah menyelesaikan transaksi, sebuah blok masuk ke blockchain sebagai database permanen. Jika sebuah blok diselesaikan, blok baru ditambahkan dengan ini atau blok baru dihasilkan. Setiap blok membawa hash dari blok sebelumnya.

Kolaborasi dan komunikasi menggunakan teknologi semua itu dapat terjadi karena komputer merupakan bagian dari teknologi informasi dan komunikasi. [10]. Diawali dengan generasi pertama dari komputer, selanjutnya industri yang berkaitan dengan teknologi informasi terus berkembang pesat dan fenomenal. Pada saat ini pengukuran secara manual tidak bisa dilakukan dalam sistem yang menggunakan informasi yang besar. Adanya aplikasi memudahkan pencatatan, perbaikan dan penghapusan data [11]. Untuk mengendalikan proses dalam aplikasi dapat menggunakan fitness dan ukuran kinerja [12].

Elemen dan Ancaman Utama dalam Keamanan Blockchain

Inovasi dan teknologi baru semakin tumbuh karena pesatnya perkembangan teknologi [13]. *Blockchain* dapat diintegrasikan dengan *smart contract*, memastikan bahwa program dapat mengeksekusi logika preset melalui *self-limitation* dan enkripsi keamanan secara kredibel dan otomatis [14]. Gambar 1 menunjukkan, blockchain dapat mengintegrasikan beberapa teknik, seperti kriptografi, protokol jaringan P2P, dan algoritma konsensus, untuk mencapai lebih banyak fungsi sistem keamanan. Protokol jaringan P2P memungkinkan blockchain untuk menangani pola yang tidak dapat diprediksi sehingga logika bisnis tidak ketinggalan zaman [15].



Gambar 1: Elemen Dan Ancaman Utama Dalam Keamanan Blockchain

Namun, masalah keamanan di blockchain terus menjadi tantangan yang signifikan [16]. Sistem blockchain telah menderita banyak serangan luar di sekitar Internet [17]. Keamanan blockchain adalah perlindungan transaksi dalam blok terhadap ancaman internal, jahat, periferal, dan tidak disengaja. Perlindungan ini bergantung pada deteksi, pencegahan, dan respons yang tepat terhadap ancaman dari berbagai tingkat menggunakan kebijakan dan alat keamanan [17]. Namun, berbagai penelitian keamanan blockchain saat ini bersifat teknis, dengan pertimbangan terbatas pada masalah organisasi dan operasional [18]. Untuk memperbaiki kekurangan dalam sistem berbasis konten maka digunakan sistem rekomendasi [19]. Kebutuhan pengembangan digunakan karena adanya kebutuhan komponen komputer baik perangkat keras dan perangkat lunak [20].

Salah satu tahapan pengembangan sistem yaitu dengan melakukan proses dengan tujuan agar sistem dapat mengetahui kesalahan dan memperbaiki kesalahan sehingga sistem dapat berjalan sesuai rencana [21]. Manajemen berbasis model dengan fungsi analog dan pengelolaan basis data dapat dilakukan dengan menggunakan sub sistem. [22]. Kepuasan pengguna dapat dilakukan dengan analisis *online* dan evaluasi secara *offline* [23]. Tahap ini mentranslasi kebutuhan perangkat lunak dari tahap analisis kebutuhan ke representasi desain [24]. Kebutuhan pengguna dapat diketahui dengan melakukan rancangan antarmuka [20]. E-commerce sebagai penerapan dari

sistem informasi dalam proses pengembangan menggunakan *maturity model*. Dalam e-commerce terdapat kegiatan transaksi antara perusahaan dan individu [25].

Kerangka Keamanan Blockchain

Terdapat berbagai arsitektur dan model keamanan sistem, yang dapat digunakan sebagai pedoman untuk membangun kerangka kerja keamanan blockchain bisa dilihat pada Tabel 1. Pertama, tiga arsitektur pertama pada Tabel 1 menekankan implementasi dan keamanan organisasi dari suatu sistem. Arsitektur Keamanan Informasi yang diusulkan oleh Tudor berfokus pada lima komponen penting: 1) organisasi & infrastruktur, 2) kebijakan & prosedur, 3) baseline & penilaian risiko, 4) program kesadaran & pelatihan, dan 5) kepatuhan [26]. Kerangka kebijakan untuk menafsirkan risiko dalam keamanan e-Business membahas aturan kebijakan untuk mengelola informasi di antara banyak organisasi [27].

Arsitektur keamanan mengidentifikasi tuntutan untuk sebuah arsitektur terintegrasi untuk mencapai keamanan maksimum [26]. Arsitektur berikutnya yang ditawarkan oleh dua perusahaan IT yaitu, IBM konsep keamanan. IBM memberikan pandangan tentang keamanan, termasuk bisnis, teknologi, penyampaian layanan, dan perpaduan domain cenderung memiliki elemen yang sama [28]. Oracle mengusulkan arsitektur referensi yang mencakup tiga aspek penting untuk mencapai keamanan, yaitu, keamanan data, pencegahan penipuan, dan pemberdayaan kepatuhan [29]. Penerapan teknologi informasi merupakan skenario penerapan implementasi wujud nyata dari layanan pengendalian informasi.

Standar Operasi dan Peraturan

Blockchain belum matang di bidang skalabilitas, kinerja, dan interoperabilitas dengan sistem lain. Selain tantangan teknis, perusahaan menghadapi tantangan manajemen karena blockchain harus diasimilasi dalam sistem kelembagaan, peraturan, sosial, ekonomi, dan fisik yang kompleks. Platform blockchain open-source menciptakan anomali dalam mencapai pendekatan terpadu dengan standar dan kodenya sendiri. Standardisasi terminologi dan teknologi sangat penting untuk mengoptimalkan interoperabilitas model yang berbeda. Tata kelola sangat penting untuk berhasil menerapkan blockchain sambil melindungi peserta dan meningkatkan ketahanan sistem terhadap serangan keamanan siber. Transformasi

bisnis berubah menjadi digital bisnis [30]. Terlepas dari sifat self-governing dari blockchain, regulasi sistem desentralisasi masih harus diselesaikan dalam implementasi yang sebenarnya [31]. Kurangnya standar umum dan peraturan yang jelas sangat membatasi kemampuan blockchain untuk berkembang. Kurangnya standardisasi dan regulasi berarti sulit bagi praktisi untuk mengambil manfaat dari eksplorasi dan kesalahan orang lain. Selain itu, ketika pengguna memasukkan blockchain ke dalam konteks bisnis, mereka perlu mengidentifikasi model blockchain mana yang sesuai dengan kebutuhan spesifik mereka. Untuk dapat mempertahankan bisnisnya perusahaan harus beradaptasi terhadap teknologi terkini [32]. Standardisasi model lightning network dan smart contract (LNSC) untuk meningkatkan kemampuan keamanan perdagangan dalam otentikasi dan penjadwalan antara kendaraan listrik dan tumpukan pengisian daya terdistribusi. Namun, perlindungan privasi data perdagangan konsumsi tetap menjadi masalah kritis.

Efek signifikan dalam keakuratan model prediktif sudah diselidiki pada penelitian sebelumnya. [33]. Internet dan web menyediakan sejumlah besar dataset dan informasi [34]. Model dasar di dunia nyata yang berbeda dapat disesuaikan dengan dengan melakukan validasi modul [35].

Sistem dapat memanfaatkan fungsi atensi untuk pemilihan informasi yang relevan [36]. Perusahaan yang menggunakan internet untuk berbisnis harus mematuhi standar etika yang sama secara online [25]. Perencanaan idealnya dimulai dengan analisis kebutuhan, yaitu mengantisipasi keputusan masa depan ('menanyakan pertanyaan yang tepat'), yang kemudian diterjemahkan ke dalam kebutuhan informasi, yang kemudian menentukan kebutuhan data [37].

Teknik Komputasi Pada Data Blockchain Terenkripsi

Serangan, seperti serangan tabrakan, serangan primage, dan serangan terhadap dompet pengguna, memotivasi enkripsi homomorfik [38]. Enkripsi homomorfik mendukung perhitungan aljabar yang dieksekusi langsung pada ciphertext bukan plaintext, menghasilkan kerahasiaan data [39]. Mengaktifkan enkripsi homomorfik di blockchain dapat mendukung data pengguna tanpa informasi apa pun tentang diri mereka. Penggabungan blockchain dengan enkripsi homomorfik untuk melakukan e-voting tanpa pihak ketiga yang terpercaya.

Mekanisme enkripsi homomorfik penuh biasanya tidak efisien, dan dengan demikian enkripsi homomorfik parsial menarik lebih banyak perhatian dari para peneliti.

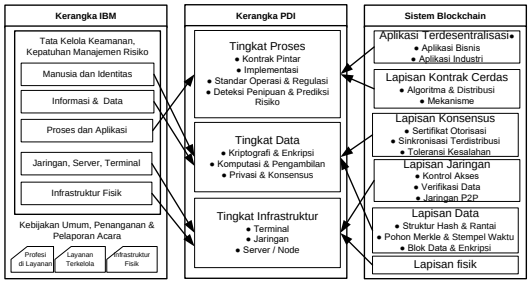
Otentikasi data dan untuk menjamin kebenaran informasi maka dapat menggunakan tanda-tangan homomorfik [40]. Ada berbagai jenis tanda tangan homomorfik, termasuk skema tanda tangan homomorfik linier, skema homomorfik polinomial, dan skema homomorfik berjenjang. Skema tanda tangan homomorfik linier dalam kriptografi berbasis identitas [41]. Saat mengintegrasikan tanda tangan homomorfik ke dalam model blockchain, perhitungan dan analisis dapat dilakukan sambil merealisasikan otentikasi data. Penggunaan pseudo-random noise generator dan privasi diferensial merupakan solusi alternatif untuk mengurangi inefisiensi dan ketidakmatangan enkripsi homomorfik. Kedalaman multiplikatif sirkuit adalah batasan praktis utama dalam kinerja sebagian besar algoritma enkripsi homomorfik. Dalam hal kelenturan, skema enkripsi homomorfik memiliki properti keamanan yang lebih lemah daripada skema non-homomorfik. Namun, mereka kekurangan skema tanda tangan full-homomorphic yang praktis dan efisien untuk blockchain selain algoritma Gentry, terutama untuk mengaktifkan keamanan dan pembelajaran mendalam dari data blockchain terdesentralisasi secara efisien. Efek signifikan dalam keakuratan model prediktif sudah diteliti pada penelitian sebelumnya [33].

METODE

Untuk mengintegrasikan arsitektur keamanan yang ada dengan aplikasi berbasis blockchain mengenai masalah teknologi dan organisasi secara seimbang [42], Penelitian ini menganalisis arsitektur keamanan blockchain infrastruktur data proses pada model PDI dengan memetakan arsitektur keamanan yang diusulkan IBM. Gambar 2 memperlihatkan kerangka PDI yang terdiri dari tiga aspek: tingkat proses, tingkat data, dan tingkat infrastruktur. Keamanan tingkat data diapit oleh proses dan infrastruktur. Keamanan blockchain di tingkat data terdiri dari otentikasi, enkripsi, algoritma konsensus, kontrol akses, dan manajemen kunci.

Tingkat proses mencakup kontrak pintar, keamanan implementasi, standar operasi, dan deteksi penipuan. Level infrastruktur mencakup perangkat terminal, jaringan, dan server super-node jika ada. Kontribusi keamanan dapat dipetakan menurut ketiga tingkatan tersebut. Tiga bagian berikutnya memeriksa sejauh mana masalah ini telah

dipelajari. Dalam sistem berbasis aturan menggunakan manajemen ketidakpastian dengan prosedur pencarian otomatis menggunakan parameter certainty faktor sebagai pengendali [43].



Gambar 2: Kerangka Keamanan Blockchain

Tiga referensi terakhir pada Tabel 1 berkonsentrasi pada standar keamanan informasi yang seragam yang diringkas dari praktik. Rangkaian standar ISO/IEC 27000 meringkas praktik terbaik manajemen keamanan yang diakui secara global [44]. Pusat Keamanan Internet membantu organisasi memfokuskan sumber daya dan keahlian keamanan mereka untuk bertahan dari serangan dunia maya [45]. Arsitektur Referensi Keamanan yang diusulkan oleh Tripwire mengintegrasikan visibilitas aset dengan fidelitas tinggi dan intelijen titik akhir yang mendalam dengan konteks bisnis, mengotomatisasi keamanan, dan operasi teknologi informasi [46].

Kerangka keamanan siber yang diusulkan oleh National Institute of Standards & Technology (NIST) menghadirkan kerangka kerja keamanan untuk memungkinkan perusahaan, meningkatkan kemampuan mereka untuk bertahan melawan serangan dunia maya [47]. Adanya perkembangan teknologi informasi menuntut perubahan pada peran yang semula hanya penyedia informasi menjadi meningkat pada peran pengambil keputusan [48]. Dalam hal aplikasi berbasis blockchain, masalah keamanan utama meliputi pembuatan dan perlindungan kunci privat, kerentanan algoritma tanda tangan, sentralisasi proses konsensus, kerentanan kontrak cerdas, dan kerentanan aplikasi terdesentralisasi,

Tabel 1: Arsitektur, Kerangka, dan Standar Keamanan.

Model	Metrik
Arsitektur Keamanan	Arsitektur terintegrasi untuk mencapai keamanan maksimum [26].
Arsitektur Referensi Keamanan	Pandangan luas tentang keamanan, termasuk bisnis, teknologi, dan layanan [28]
Konsep Keamanan	Gambaran keamanan apa yang disediakan arsitektur dan bagaimana hal itu dapat direalisasikan [29].
ISO/IEC 27000	Rangkuman praktik terbaik manajemen keamanan [44].
Kontrol Keamanan Kritis	Membantu organisasi memfokuskan sumber daya dan keahlian keamanan mereka [49].
Keamanan Siber	Kerangka kerja untuk memungkinkan organisasi meningkatkan kemampuan [47]
ISA	Memandu pelaksana untuk mengembangkan arsitektur keamanan yang efektif [50].

Sumber: [26], [28], [29], [44], [47], [50]

HASIL DAN PEMBAHASAN

Masalah keamanan smart contract terjadi dalam tiga level, yaitu level bisnis, level mesin virtual, dan level kode kontrak. Secara khusus, masalah keamanan tingkat bisnis mencakup akses tidak sah, infeksi program jahat,

keadaan yang tidak dapat diprediksi, dan ketergantungan pemesanan transaksi. Masalah keamanan tingkat mesin virtual termasuk batas ukuran tumpukan, menghasilkan keacakan, dan kendala waktu.

Hasil

Proses bisnis mengharuskan praktisi untuk memutuskan dan mematuhi kebijakan yang dapat diberlakukan oleh peserta untuk menjaga keamanan sistem mereka. Keamanan blockchain pada tingkat proses sangat rumit karena banyak tugas dan tata kelola. Pada banyak elemen sederhana terjadi pengolahan informasi [51]. Kinerja aplikasi yang baru dilakukan perbandingan dengan aplikasi yang ada sebagai bagian dari implementasi sistem [43]. Masalah keamanan *smart contract* terjadi dalam tiga level, yaitu level bisnis, level mesin virtual, dan level kode kontrak. Secara khusus, masalah keamanan tingkat bisnis mencakup akses tidak sah, infeksi program jahat, keadaan yang tidak dapat diprediksi, dan ketergantungan pemesanan transaksi. Masalah keamanan tingkat mesin virtual termasuk batas ukuran tumpukan, menghasilkan keacakan, dan kendala waktu. Keamanan tingkat kode dari kontrak pintar adalah masalah penting untuk aplikasi blockchain [42].

Volume transaksi yang terlibat dalam kontrak pintar di blockchain sangat besar, dan diperlukan skenario yang lebih praktis untuk menguji stabilitas sistem guna menemukan potensi kerentanan kode. Strategi transformasi organisasi dipengaruhi oleh transformasi digital dalam banyak hal dan tergantung pula pada pemangku kepentingan [49].

Kontrak pintar dapat diterapkan dalam situasi yang lebih kompleks, dan kompleksitas serta kesulitan teknis dari kode kontrak juga dapat meningkat. Masalah keamanan tingkat kode yang khas dari kontrak termasuk panggilan ke yang tidak diketahui, pengiriman tanpa gas, dan keadaan buntu [44]. Reentrancy dan keadaan yang tidak dapat diprediksi juga merupakan kerentanan kode yang umum [48]. Kegagalan untuk menyandikan mesin status yang benar (misalnya, lalai memeriksa status saat ini dan menghilangkan transisi tertentu) adalah masalah yang paling sering diamati.

Kontrol akses menjadi lebih rumit dalam mengembangkan sistem informasi dari sistem terintegrasi menjadi aplikasi terdistribusi, berbasis cloud, dan berbasis blockchain. Teknologi yang terkait dengan tampilan informasi tentang dunia sekitar pengguna dan cara mengendalikannya [52]. Penggunaan big data, aplikasi pada telepon pintar, dan aplikasi berbasis web merupakan contoh dari pemanfaatan teknologi informasi [53]. Dalam penelitian blockchain, kontrol akses halus dari data terdesentralisasi biasanya dipertahankan dengan menggabungkan kontrak pintar dan skema Enkripsi Berbasis Atribut (ABE). Kontrak pintar dapat menyimpan ciphertext ABE yang diperbarui, mengekspresikan semantik logika otorisasi, dan secara fleksibel menentukan kebijakan kontrol akses untuk

menghapus dan mengedit data. Baru-baru ini, para sarjana mencoba menggabungkan kontrak pintar dengan model pembelajaran mesin untuk menyediakan kontrol akses (otorisasi) yang otomatis, dinamis, dioptimalkan, dan disesuaikan sendiri [54].

Pembahasan

Peluang organisasi untuk mendapatkan informasi dalam menunjang kegiatan operasinya dapat dilakukan dengan memanfaatkan big data. [4]. Sebagian besar konten tekstual kini telah tersedia dan diperlukan teknik untuk menggunakan informasi tersebut secara bermakna dengan mengisolasi dan memeriksanya. [55]. Algoritma deep learning dan teknologi big data berguna untuk pemrosesan data dan keamanan IoT [7]. Perbedaan dan kesamaan target dipengaruhi oleh tingkat perlindungan. [11].

Terlepas dari aplikasi Fintech berbasis *cryptocurrency* dan blockchain yang terkenal, ada banyak sektor implementasi blockchain dalam konteks *Internet of Things* (IoT), ekonomi bersama, sistem perawatan kesehatan, kota pintar, jaringan pintar, manufaktur sosial, dan rantai pasokan manajemen dalam pelayanan sosial. Akibatnya, ada banyak risiko saat mengimplementasikan blockchain. Integrasi blockchain dengan sistem yang ada dapat menimbulkan tantangan besar dalam bisnis nyata. Implementasi keamanan yang tinggi membutuhkan pengujian kode kritis yang ketat. Model bisnis asli mungkin tidak sesuai dengan logika bisnis yang mendukung blockchain karena realisasi keamanan sangat berkorelasi dengan lingkungan penerapan.

Internet of Things (IoT) adalah teknologi penting yang memungkinkan interaksi perangkat untuk bertukar data untuk pengambilan keputusan yang cerdas. Namun, kurangnya penanggulangan keamanan membuat jaringan IoT rentan terhadap ancaman dan serangan dunia maya, yang berdampak pada perlindungan privasi pemangku kepentingan yang terlibat. Sulit untuk membuat sistem otentikasi terpusat karena skala data yang sangat besar dan tingginya biaya pemeliharaan server untuk IoT. Kemampuan blockchain, termasuk tamper-resisting, transparansi, kemampuan audit, dan ketahanan jaringan, dapat mengubah kekurangan arsitektur IoT terpusat dan jaringan industri. Dengan perangkat heterogen mulai dari sensor hingga server, arsitektur keamanan multi-lapisan yang dapat diadaptasi secara dinamis dapat dirancang dengan standarisasi cerdas dari perangkat jaringan IoT. Protokol yang diterapkan, bersama dengan mekanisme konversi, perlu beroperasi di berbagai lapisan jaringan IoT.

Data berperan sebagai fondasi bangunan sebuah informasi [56]. Peningkatan pelayanan dalam sistem informasi ditunjang oleh aplikasi dengan sistem basis data yang baik [57]. Model analisis yang ada belum mampu

untuk menyelesaikan permasalahan pada domain [58].

SIMPULAN

Penelitian ini menganalisis arsitektur keamanan blockchain pada infrastruktur data proses, dan membahas lanskap masalah keamanan blockchain dan menguraikan peluang penelitian dalam sistem dan layanan informasi. Keamanan blockchain dikategorikan menjadi tiga tingkatan, yaitu tingkat proses, tingkat data, dan tingkat infrastruktur, yang disebut sebagai model keamanan blockchain PDI. Penelitian ini juga mengkaji sejauh mana aspek keamanan ini telah ditangani. Berdasarkan wawasan yang diperoleh dari analisis masalah penelitian, arah penelitian yang menjanjikan untuk keamanan blockchain telah diuraikan. Ditemukan bahwa penelitian ini telah mencerminkan kemajuan konseptual dan teknis yang signifikan di bidang keamanan blockchain, dan diharapkan dengan meletakkan dasar yang kuat untuk membuat keamanan blockchain, semoga hasil penelitian ini bermanfaat dalam bidang rekayasa layanan teknologi blockchain.

DAFTAR PUSTAKA

[1] Y. Yuan, S. Member, and F. Wang, "Blockchain and Cryptocurrencies : Model , Techniques , and Applications," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 48, no. 9, pp. 1421–1428, 2018.

[2] J. L. Zhao, S. Fan, and J. Yan, "Overview of business innovations and research opportunities in blockchain and introduction to the special issue," *Financ. Innov.*, vol. 2, no. 1, pp. 1–7, 2016.

[3] N. I. Putri, R. Komalasari, and Z. Munawar, "Pentingnya Keamanan Data dalam Intelijen Bisnis," *J-SIKA| J. Sist. Inf. Karya Anak Bangsa*, vol. 2, no. 2, pp. 41–48, 2020.

[4] Z. Munawar and N. Indah Putri, "Keamanan Jaringan Komputer Pada Era Big Data," *J-SIKA|Jurnal Sist. Inf. Karya Anak Bangsa*, vol. 2, no. 1, pp. 14–20, Jul. 2020.

[5] Z. Munawar *et al.*, "Aplikasi Pendeteksi dan Pelacakan Kendaraan Menggunakan Jaringan Neural Propagasi Balik," *Infotech*, vol. 8, no. 2, pp. 135–140, 2022.

[6] Z. Rubiyanto, R. Komalasari, Z. Munawar, and N. I. Putri, "Sistem Monitoring Project Berbasis Web di PT. Hariff Daya Tunggal Engineering," *Pros. SISFOTEK*, vol. 6, no. 1, pp. 21–27, 2022.

[7] Z. Munawar and N. I. Putri, "Keamanan IoT Dengan Deep Learning dan Teknologi Big Data," *Temat. - J. Teknol. Inf. dan Komun.*, vol. 7, no. 2, pp. 161–185, Dec. 2020.

[8] Z. Munawar, "Machine Learning Approach for Analysis of Social Media," *ADRI Int. Journal. Information. Technol*, vol. 1, no. 1, pp. 5–8, 2017.

[9] N. I. Putri, Z. Munawar, and R. Komalasari, "Minat Penggunaan QRIS Sebagai Alat Pembayaran Pasca Pandemi," *Pros. SISFOTEK*, vol. 6, no. 1, pp. 155–160, 2022.

[10] Z. Munawar and D. Z. Musadad, "Penggunaan TIK untuk Bidang Pendidikan," in *Munuju Masyarakat Madani*, 2015, pp. 555–563.

[11] Z. Munawar, "Mekanisme keselamatan, keamanan dan keberlanjutan untuk sistem siber fisik," *J. Teknol. Inf. Dan Komun.*, vol. 7, no. 1, pp. 58–87, 2020.

[12] N. Ramsari and Z. Munawar, "Pengambilan Keputusan Dengan Teknik Soft Computing," *J. Ilm. Teknol. Inf. Terap.*, vol. 2, no. 3, pp. 244–253, 2016.

[13] D. Khairunnisa, A. D. Rachmanto, Z. Munawar, and M. Haitan, "Aplikasi Virtual Tour Dinamis Pada Universitas Nurtanio Bandung Berbasis Web," in *SNASIKOM*, 2022, no. 1, pp. 42–50.

[14] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Applied Innovation Review," *Appl. Innov. Rev.*, vol. 9, no. 2016, pp. 1–16, 2016.

[15] I. O. Pappas, P. Mikalef, M. N. Giannakos, J. Krogstie, and G. Lekakos, "Towards digital transformation and sustainable societies," *Inf. Syst. E-bus. Manag.*, vol. 16, no. 3, pp. 479–491, 2018.

[16] H. N. Higgins, "Corporate system security : towards an integrated management approach," *Inf. Manag. Comput. Secur.*, vol. 7, no. 5, pp. 217–222, 1999.

[17] M. T. Siponen and H. Oinas-kukkonen, "Information Security Issues and Respective Contributions," vol. 38, no. 1, pp. 60–80, 2007.

[18] T. T. Huynh, "A Survey on Security and Privacy Issues of Blockchain Technology," in *2019 International Conference on System Science and Engineering (ICSSE)*, 2019, pp. 362–367.

[19] Z. Munawar, N. Suryana, Z. B. Sa'aya, and Y. Herdiana, "Framework With An Approach To The User As An Evaluation For The Recommender Systems," in *2020 Fifth International Conference on Informatics and Computing (ICIC)*, 2020, pp. 1–5.

[20] Z. Munawar, M. I. Fudsyi, and D. Z. Musadad, "Perancangan Interface Aplikasi Pencatatan Persediaan Barang Di Kios Buku Palasari Bandung Dengan Metode User Centered Design Menggunakan Balsamiq Mockups," *J. Inform.*, vol. 6, no. 2, pp. 10–20, 2019.

[21] Z. Munawar, "Aplikasi Registrasi Seminar Berbasis Web Menggunakan QR Code pada Universitas XYZ," *Temat. J. Teknol. Inf. Dan Komun.*, vol. 6, no. 2, pp. 68–77, 2019.

[22] Z. Munawar, "Penerapan Metode Analytical Hierarchy Process Dan Technique For Order Preference By Similarity To Order Solution Dalam Seleksi Penerimaan Mahasiswa Baru Jalur Bidik Misi," *Temat. - J. Teknol. Inf. dan Komun.*, vol. 4, no. 1, pp. 34–53, Jun. 2017.

[23] N. I. Putri, Y. Herdiana, and Z. Munawar, "Meningkatkan Rekomendasi Menggunakan Algoritma Perbedaan Topik," *J-SIKA| J. Sist. Inf. Karya Anak Bangsa*, vol. 02, no. 02, pp. 17–26, 2020.

[24] I. Rahmawati, Z. Munawar, R. Komalasari, and N. I. Putri, "Sistem Informasi Manajemen Kepegawaian di Universitas Nurtanio," in *Sistem Informasi dan Teknologi - SISFOTEK 6*, 2022, pp. 10–20.

[25] Z. Munawar, "Keamanan Pada E-Commerce Usaha Kecil dan Menengah," *Tematik*, vol. 5, no. 1, pp. 1–16, 2018.

[26] J. H. P. Eloff and M. M. Eloff, "Information security architecture," in *Computer Fraud & Security*, 2005, no. November, pp. 10–16.

[27] J. Rees, S. Bandyopadhyay, and E. H. Spafford, "PFIRES: A policy framework for information security," *Commun. ACM*, vol. 46, no. 7, pp. 101–106, 2003.

[28] J. Darwin, "Security Reference Architecture," in *AWS RA*, 2010, p. 1.

[29] Oracle, "Security in Depth Reference Architecture," in *Oracle Enterprise Transformation Solutions Series*, 2013, no. March, pp. 1–27.

[30] P. Pramesti, A. Dwijayanti, R. Komalasari, and Z. Munawar, "Transformasi Bisnis Digital UMKM Bola Ubi Kopong di Masa Pandemi Covid-19," *ATRABIS J. Adm. Bisnis*, vol. 7, no. 2, pp. 112–119, Dec. 2021.

[31] G. W. Peters and E. P. Chapelle, "Trends in Cryptocurrencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective," in *Journal of Financial Perspectives*, 2015, pp. 92–113.

[32] P. Pramesti, A. Dwijayanti, R. Komalasari, Z. Munawar, and B. Harto, "Review Penelitian Bisnis dan Metaverse menggunakan Teknik Bibliometrik," *ATRABIS J. Adm. Bisnis*, vol. 8, no. 1, pp. 1–7, Jun. 2022.

[33] Z. Munawar, "Penggunaan Profil Media Sosial Untuk Memprediksi Kepribadian," *Temat. - J. Teknol. Inf. dan Komun.*, vol. 4, no. 2 SE-Articles, pp. 18–37, Dec. 2017.

[34] Z. Munawar, Rustiyana, Y. Herdiana, and N. I. Putri, "Sistem Rekomendasi Hibrid Menggunakan Algoritma Apriori Mining Asosiasi," *Temat. - J. Teknol. Inf. dan Komun.*, vol. 8, no. 1, pp. 69–80, Jun. 2021.

[35] N. I. Putri, Rustiyana, Y. Herdiana, and Z. Munawar, "Sistem Rekomendasi Hibrid Pemilihan Mobil Berdasarkan Profil Pengguna dan Profil Barang," *Temat. - J. Teknol. Inf. dan Komun.*, vol. 8, no. 1 SE-Articles, pp. 56–68, Jun. 2021.

[36] N. I. Putri and Z. Munawar, "Mekanisme umum untuk sistem kecerdasan buatan," *Comput. J. Inform.*, vol. 06, pp. 58–75, 2019.

[37] T. H. Davenport, "Business Intelligence and Organizational Decisions," *Int. J. Bus. Intell. Res.*, vol. 1, no. 1, pp. 1–12, 2010.

[38] S. Yaji, K. Bangera, and B. Neelima, "Privacy Preserving in Blockchain based on Partial Ho- momorphic Encryption System for AI Applications," in *2018 IEEE 25th International Conference on High Performance Computing Workshops (HiPCW)*, 2018, pp. 81–85.

[39] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public- Key Cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[40] R. Jhonson, D. Molnar, D. Song, and D. Wagner, "Homomorphic signature schemes," in *Topics in Cryptology*, 2002, pp. 1–18.

[41] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, vol. 6, no. 2, pp. 1–8, 2018.

[42] D. Treek, "An integral framework for information systems security management," *Comput. Secur.*, vol. 22, no. 4, pp. 337–360, 2003.

[43] N. Indah Putri, "Sistem Pakar Diagnosa Tingkat Kecanduan Gadget Pada Remaja Menggunakan Metode Certainty Factor," *UIN J.*, vol. 53, no. 4, p. 130, 2018.

[44] I. ISO, "Information security management systems," in *ISO/IEC 27000 family*, 2013, p. 1.

[45] CIS, "CIS Critical Security Controls," in *Center Information Security*, 2017, p. 1.

[46] M. D, "Security Reference Architecture: A Practical Guide to Implementing Foundational Controls." p. 1, 2017.

[47] NIST, "Cybersecurity Framework," in *National Institute of Standards & Technology*, 2018, p. 1.

[48] N. Indah Putri, M. Ismirani Fudsy, D. Karmana, S. Muda Nasution, Z. Munawar, and B. Lesmana, "Peran Akuntan Dengan Kompetensi Teknologi Informasi Pada Umkm Di Era Globalisasi," *J. Ris. Akunt. dan*

Bisnis, vol. 8, no. 2, pp. 208–221, 2022.

[49] N. I. Putri, Iswanto, A. Dwijayanti, R. Komalasari, and Z. Munawar, "Penerapan Model Maturitas Digital Pada Kinerja Startup," *Temat. J. Teknol. Inf. Komun.*, vol. 9, no. 1, pp. 61–69, 2022.

[50] J. Tudor, *Information Security Architecture*. Auerbach Publishers, 2000.

[51] Z. Munawar, "Perkembangan Riset di Bidang Neurocomputing," *Temat. - J. Teknol. Inf. dan Komun.*, vol. 2, no. 2, pp. 17–31, Dec. 2015.

[52] Iswanto, N. I. Putri, D. Widhiantoro, Z. Munawar, and R. Komalasari, "Pemanfaatan Metaverse Di Bidang Pendidikan," *Temat. J. Teknol. Inf. Komun.*, vol. 9, no. 1, pp. 44–52, Jun. 2022.

[53] Z. Munawar, "Manfaat Teknologi Informasi di Masa Pandemi Covid-19," *J-SIKA|Jurnal Sist. Inf. Karya Anak Bangsa*, vol. 3, no. 2, pp. 53–63, Dec. 2021.

[54] A. Outchakoucht, H. Es-Samaali, and J. Philippe, "Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 7, pp. 417–424, Jan. 2017.

[55] Z. Munawar, Iswanto, D. Widhiantoro, and N. I. Putri, "Analisis Sentimen Covid-19 Pada Media Sosial Dengan Model Neural Machine Translation," *Temat. J. Teknol. Inf. Komun.*, vol. 9, no. 1, pp. 15–20, 2022.

[56] Z. Munawar, B. Siswoyo, and N. S. Herman, "Machine learning approach for analysis of social media," *ADRI Int. Journal. Information. Technol.*, vol. 1, pp. 5–8, 2017.

[57] Z. Munawar, "Perbaikan Teknis Sistem Pencatatan Persediaan Barang Berbasis Komputer Bagi Pedagang Buku Pasar Palasari Kota Bandung Menghadapi Era Pasar Kompetitif," *JAST J. Apl. Sains dan Teknol.*, vol. 4, no. 1, p. 52, 2020.

[58] Z. Munawar, "Research developments in the field neurocomputing," in *Proceedings of 2016 4th International Conference on Cyber and IT Service Management, CITSM 2016*, 2016, no. 59, pp. 1–6.