JIMU: Jurnal Ilmiah Multi Disiplin
Vol. 04, No. 01, Tahun 2025, Hal. 568-578, ISSN: 3031-9498 (Online)

Analisis Peran *Blockchain* dalam *Zero-Trust Architecture* untuk Penguatan Identitas Digital dan Privasi Data

Fernando Hose[1], Florika Censaka[2], Ricky Andrian Wijaya[3], Jennifer[4], Chrystina Tanuwijaya[5], Joosten Ng[6]
[1,2,3,4,5,6] Fakultas Informatika, Universitas Mikroskil
Jalan Thamrin No 140, Medan, Sumatera Utara, telp 0614573767
E-mail: 221120176@students.mikroskil.ac.id

Article Info

Article history:
Received September 22, 2025
Revised September 27, 2025
Accepted September 30, 2025

Keywords:
Blockchain, Zero-Trust Architecture, Digital Identity, Data Privacy

ABSTRACT

The rapid growth of the digital era has intensified risks to digital identity and data privacy, demanding more adaptive security mechanisms. Zero-Trust Architecture (ZTA), with its principle of "never trust, always verify", ensures strict access verification, while blockchain offers a decentralized, transparent, and tamper-resistant system. This study aims to analyze the role of blockchain in strengthening ZTA, particularly in authentication and identity management. Using a qualitative case study approach with literature and document analysis, the findings indicate that the adoption of Decentralized Identifiers (DID) and Self-Sovereign Identity (SSI) enables users to control their personal data while enhancing auditability, multi-layer verification, and privacy through smart contracts and zero-knowledge proofs. However, integrating blockchain into ZTA still faces challenges, including scalability, key management, and regulatory compliance. Therefore, hybrid approaches and adaptive regulations are required for blockchain–ZTA integration to serve as a reliable and sustainable foundation for digital security governance.

Article Info

Article history:
Received September 22, 2025
Revised September 27, 2025
Accepted September 30, 2025

Keywords:
Blockchain, *Zero-Trust Architecture*, Identitas Digital, Privasi Data

ABSTRAK

Perkembangan era digital meningkatkan risiko terhadap identitas digital dan privasi data, sehingga dibutuhkan mekanisme keamanan yang lebih adaptif. *Zero-Trust Architecture* (ZTA) hadir dengan prinsip "*never trust, always verify*", sementara *blockchain* menawarkan sistem desentralisasi yang transparan dan tahan manipulasi. Kajian ini bertujuan menganalisis peran *blockchain* dalam memperkuat ZTA, khususnya pada aspek autentikasi dan pengelolaan identitas. Melalui pendekatan kualitatif berbasis studi kasus dengan analisis literatur dan dokumen, hasil menunjukkan bahwa penerapan *Decentralized Identifiers* (DID) dan *Self-Sovereign Identity* (SSI) memungkinkan pengguna mengendalikan data pribadi, serta memperkuat auditabilitas, verifikasi berlapis, dan privasi melalui *smart contract* serta *zero-knowledge proofs*. Namun, integrasi *blockchain*-ZTA masih menghadapi tantangan berupa skalabilitas, manajemen kunci, dan kepatuhan regulasi. Oleh karena itu, diperlukan pendekatan *hybrid* dan regulasi yang adaptif agar integrasi ini dapat menjadi fondasi keamanan digital yang andal dan berkelanjutan.

Corresponding Author:
Fernando Hose
Universitas Mikroskil
E-mail: 221120176@students.mikroskil.ac.id

PENDAHULUAN

Di era digital saat ini, keamanan siber menjadi salah satu aspek yang sangat penting untuk diperhatikan. Identitas digital dari individu, organisasi maupun pemerintahan mencakup informasi pribadi, kontak dan preferensi individu, sering menjadi target dari serangan siber atau penyalahgunaan oleh pihak yang tidak bertanggung jawab (Kriswandaru et al., 2025). Hal tersebut dapat terjadi karena digitalisasi telah memungkinkan pengumpulan, penyimpanan, dan pengolahan data yang lebih mudah, cepat, dan terpusat (Suryawijaya, 2023).

Konsep *Zero-Trust Architecture* (ZTA) diperkenalkan dengan prinsip "*never trust, always verify*". Setiap pengguna, perangkat, maupun aplikasi baik yang berasal dari dalam maupun luar organisasi diverifikasi secara ketat sebelum memperoleh akses. ZTA mengandalkan mekanisme *policy enforcement point* dan *zero-trust engine* untuk memastikan setiap permintaan akses memenuhi parameter keamanan yang telah ditentukan (Singh et al., 2024). Di sisi lain, *Blockchain* menawarkan solusi desentralisasi yang dapat memperkuat prinsip ZTA. Sebagai buku besar digital terdistribusi, *blockchain* bersifat kekal dan transparan, sehingga setiap catatan transaksi atau identitas tidak dapat diubah tanpa konsensus jaringan sehingga menjadikan teknologi *blockchain* sebagai salah satu solusi potensial dalam penguatan identitas dan privasi data (Singh et al., 2024).

Studi-studi terbaru, seperti yang dilakukan oleh (Chaudhry & Hydros, 2023), mengusulkan kerangka kerja berdasarkan konsep *Zero-Trust* dan teknologi *blockchain* dengan fokus untuk melindungi sektor perbankan dari serangan siber dan kebocoran data. Kombinasi antara teknologi *blockchain* dan ZTA terbukti dapat meningkatkan keamanan data dari serangan siber karena kombinasi antara ZTA dan *blockchain* memberikan potensi besar dalam penguatan identitas digital dan perlindungan privasi data. ZTA memastikan bahwa setiap akses diverifikasi secara ketat, sementara *blockchain* menjamin keaslian, integritas, dan kontrol penuh terhadap data identitas.

Meski demikian, penerapan *blockchain* dalam kerangka ZTA untuk mendukung penguatan identitas digital dan privasi data masih menghadapi berbagai tantangan, baik dari aspek teknis maupun regulasi. Tujuan dari penelitian ini adalah untuk menganalisis peran teknologi *blockchain* dalam memperkuat penerapan ZTA, khususnya dalam menjamin keaslian identitas digital serta melindungi privasi data pengguna. Kajian ini penting mengingat masih terbatasnya penelitian komprehensif yang menyoroti integrasi *blockchain* dengan ZTA dalam konteks keamanan identitas dan data. Hasil penelitian diharapkan dapat memberikan kontribusi bagi pengembangan kebijakan serta strategi keamanan digital yang lebih adaptif dan terpercaya.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan menerapkan metodologi studi kasus. Studi kasus dipilih untuk memberikan kajian mendalam mengenai penerapan teknologi *blockchain* dan kerangka ZTA untuk penguatan identitas digital dan privasi data. Penelitian ini juga didasarkan pada desain studi kasus deskriptif yang bertujuan untuk memberikan gambaran komprehensif mengenai peran teknologi *blockchain* dalam *Zero-Trust Architecture* untuk penguatan identitas digital dan privasi data. Pendekatan ini memungkinkan peneliti mempelajari fenomena dalam situasi dunia nyata dan mencapai pemahaman yang mendalam.

Data diperoleh melalui dua sumber utama, yaitu tinjauan pustaka yang mencakup artikel jurnal, konferensi, dan buku terkini yang membahas konsep *Zero-Trust Architecture* (ZTA), teknologi *blockchain*, identitas digital, privasi data, serta isu keamanan siber secara umum. Selanjutnya dilakukan analisis dokumen berupa regulasi, kebijakan, laporan penelitian, serta pedoman yang dikeluarkan pemerintah, organisasi, maupun asosiasi industri terkait implementasi ZTA dan *blockchain* di bidang keamanan identitas dan privasi data. Materi tersebut diperoleh dari publikasi akademik maupun sumber resmi seperti situs web pemerintah dan lembaga terkait.

Data yang terkumpul akan dianalisis melalui pendekatan tematik seperti mengklasifikasikan dan mengindentifikasikan tema-tema utama dari tinjauan literatur dan analisis dokumen, yang kemudian dilanjutkan dengan analisis silang dan sintesis data dari berbagai sumber untuk mendapatkan pemahaman komprehensif (Wendelborn et al., 2023). Lalu pada tahap akhir dilakukan penafsiran terhadap hasil penelitian serta penarikan kesimpulan. Analisis data akan dilakukan dengan perangkat lunak pengolah data kualitatif seperti NVivo dan Atlas.ti yang berguna untuk memfasilitasi pengkodean, visualisasi dan klasifikasi data (Allsop et al., 2022)(Choe et al., 2022).

Untuk menjamin validitas dan reliabilitas hasil penelitian dilakukan beberapa langkah seperti Triangulasi data-data berbeda untuk memverifikasi dan memperkaya hasil, Audit Trail yaitu mendokumentasikan secara terperinci setiap proses pengumpulan, analisis maupun interpretasi data secara transparan agar dapat diaudit (Carcary, 2020) dan untuk tahap akhir dapat dilakukan *Peer Check* yang melibatkan rekan peneliti dalam tinjauan kritis terhadap proses dan temuan penelitian. Kerangka penelitian diharapkan dapat memberikan analisis yang komprehensif dan andal mengenai peran teknologi *blockchain* dalam *Zero-Trust Architecture* (ZTA) untuk penguatan identitas digital dan privasi data.

HASIL DAN PEMBAHASAN

Penerapan Blockchain sebagai Fondasi Zero-Trust Architecture

Zero-Trust Architecture (ZTA) dibangun atas prinsip *never trust*, *always verify*, yaitu setiap entitas harus diautentikasi dan diotorisasi secara berkelanjutan tanpa mengandalkan kepercayaan implisit. Tantangan utama penerapan ZTA terdapat pada pengelolaan identitas digital, mekanisme verifikasi yang dapat diaudit, serta kontrol akses yang konsisten lintas domain. *Blockchain* menawarkan solusi sebagai fondasi dengan menyediakan buku besar terdistribusi (*distributed ledger*) yang transparan, tahan manipulasi, serta mendukung integrasi identitas desentralisasi (*decentralized identity*) (Horne, 2025).

Penggunaan *Self-Sovereign Identity* (SSI) berbasis *blockchain* memungkinkan individu mengendalikan identitas digital mereka melalui digital wallet dan *verifiable credentials*. Elemen seperti *Decentralized Identifiers* (DIDs), skema kredensial, dan registri revokasi dicatat di ledger, sementara data sensitif tetap tersimpan *off-chain* pada pihak pemilik. Pendekatan ini mendukung prinsip minimisasi data dan verifikasi tanpa kepercayaan terpusat, yang merupakan elemen fundamental dalam ZTA (Pava-Díaz et al., 2024).

Selain itu, *blockchain* mendukung otomatisasi kebijakan keamanan melalui *smart contract* yang dapat menegakkan aturan akses, mengelola revokasi, serta mencatat jejak audit secara terdistribusi. Studi terbaru dalam konteks IoT dan jaringan 6G menunjukkan bahwa kombinasi *blockchain* dengan *inner-product encryption* dan arsitektur *Zero-Trust* mampu meningkatkan ketahanan sistem terhadap serangan lateral serta mengurangi ketergantungan pada satu titik kegagalan (Nie et al., 2025).

Implementasi nyata, seperti MediLinker pada sektor kesehatan, menunjukkan efektivitas *blockchain* dalam memperkuat privasi, auditabilitas, dan kontrol pengguna atas identitas mereka dalam kerangka ZTA (Harrell et al., 2022). Selain itu, sebuah survei komprehensif mengenai solusi *blockchain* untuk IoT mengonfirmasi bahwa teknologi ini menawarkan potensi signifikan dalam hal keamanan, privasi, serta manajemen identitas terdistribusi. Namun, studi tersebut juga menekankan adanya tantangan praktis seperti isu skalabilitas, *overhead* komunikasi, dan keterbatasan sumber daya perangkat IoT — yang semuanya harus dipertimbangkan ketika *blockchain* dijadikan fondasi ZTA (Enaya et al., 2025).

Di luar ekosistem IoT, penelitian lain mengungkap bahwa penerapan identitas terdesentralisasi berbasis DID juga mulai diintegrasikan ke dalam ekosistem metaverse dan pendidikan. Hal ini menegaskan bahwa interoperabilitas, standarisasi, dan skalabilitas menjadi kunci keberhasilan penerapan *blockchain* dalam kerangka *Zero-Trust* (Polychronaki et al., 2024). Selanjutnya, inovasi seperti penggunaan *Decentralized Identifiers* (DID) yang dipadukan dengan *Soulbound Tokens* (SBT) dan *Zero-Knowledge Proofs* (ZKP) semakin memperkuat mekanisme autentikasi berbasis *blockchain* dengan menjamin privasi pengguna dalam lingkungan digital baru seperti avatar dan Web3 (Kim & Ryou, 2023).

Selain itu, aspek perlindungan data dan identitas digital dalam konteks big data juga telah diteliti. Sebuah studi menegaskan bahwa *blockchain* dapat menjadi dasar bagi model manajemen identitas yang memadukan prinsip *Zero-Trust* dengan proteksi data dalam skala besar, termasuk pada kolaborasi antara pemerintah dan institusi swasta. Pendekatan ini menawarkan kerangka kerja keamanan informasi yang adaptif terhadap kebutuhan lintas organisasi dan skenario pertukaran data kompleks (Wang et al., 2024).

Pengelolaan Identitas Digital Berbasis Decentralized Identifiers (DID)

Decentralized Identifiers (DIDs) merupakan standar identitas digital yang memungkinkan identitas yang terdesentralisasi dan bersifat *self-sovereign*, di mana pemilik identitas memiliki kontrol penuh terhadap identitas dan data pribadinya. Dengan DIDs, identitas tidak lagi tergantung pada otoritas pusat, dan DID *Document* menyediakan material kriptografi (seperti *public key* dan *service endpoints*) untuk verifikasi. DID dan *Verifiable Credentials* (VC) yang menjadi bagian dari paradigma ini menjadi fondasi untuk mengurangi eksposur data dan memastikan verifikasi kontinu sesuai prinsip *Zero-Trust*. Referensi terkini

menjelaskan bahwa era identitas digital telah beranjak dari model terpusat ke terdesentralisasi, didorong oleh kebutuhan privasi, interoperabilitas, dan kendali pengguna terhadap data mereka sendiri (Mazzocca et al., 2025).

Integrasi teknis meliputi beberapa aspek: penggunaan *multi-party issuance* untuk mengurangi *single point of failure*; mekanisme *revocation* dan pembaharuan status identitas yang efisien; serta arsitektur yang mendukung verifikasi identitas secara otomatis dan terdistribusi tanpa bergantung pada infrastruktur tradisional PKI. Analisis studi terbaru menekankan perlunya mekanisme *distributed key generation* dan solusi *revocation* yang *scalable* agar DID dapat dioperasikan dalam skenario *Zero-Trust* pada skala produksi (Schumm et al., 2025).

Terdapat risiko dan tantangan yang harus diperhatikan: manajemen kunci privat termasuk *recovery* bila hilang; interoperabilitas antar metode DID yang berbeda yang masih rendah; latensi atau biaya tinggi bila *anchoring* atau resolusi DID dilakukan di *ledger* publik; serta tantangan *revocation* dan pembaruan status *credential* agar verifikasi tetap *fresh*. Studi desain aspek sistem identitas desentralisasi menunjukkan bahwa arsitektur penyimpanan (*storage layer*) serta pemilihan metode *anchoring* harus mempertimbangkan *trade-off* antara keamanan, privasi, dan performa agar sistem tetap efisien dan dapat diadopsi secara luas (Butincu & Alexandrescu, 2024).

Selain aspek teknis tersebut, penguatan DID juga didukung oleh inovasi dalam otentikasi multipihak. Pendekatan berbasis *signature-less verifiable credentials* memungkinkan proses verifikasi identitas dilakukan tanpa bergantung pada tanda tangan digital tradisional, sehingga dapat menyembunyikan identitas penerbit sekaligus memperkuat privasi pengguna. Model ini terbukti relevan untuk lingkungan *Zero-Trust* yang menuntut verifikasi berlapis tanpa mengurangi efisiensi sistem (Xie et al., 2025).

Di sisi lain, governansi dari *ledger-anchored* DID memainkan peranan penting untuk memastikan keadilan distribusi kontrol dalam jaringan identitas terdesentralisasi. Melalui mekanisme ini, kontrol atas DID Document dapat didelegasikan secara aman sehingga tidak ada entitas tunggal yang mendominasi. Strategi ini memperkuat prinsip *never trust*, *always verify* dengan menambahkan lapisan akuntabilitas dalam pengelolaan identitas digital (Garzon et al., 2025).

Terakhir, perlindungan privasi dalam ekosistem DID dapat ditingkatkan dengan pendekatan hibrida yang memadukan penyimpanan *off-chain* dan *zero-knowledge proofs* (ZKPs). Model ini memungkinkan pengguna hanya mengungkapkan informasi minimum yang diperlukan dalam proses verifikasi, sekaligus menjaga data personal tetap terlindungi. Pendekatan hibrida ini memberikan keseimbangan antara skalabilitas, efisiensi, dan privasi, yang menjadikannya relevan dalam implementasi *Zero-Trust* pada sistem identitas modern (Mandinyenya & Malele, 2025).

Perlindungan Privasi melalui Self-Sovereign Identity (SSI)

Self-Sovereign Identity (SSI) menjadi paradigma baru dalam pengelolaan identitas digital yang menempatkan individu sebagai pengendali utama data pribadinya. Menurut Krul et al., SSI dibangun atas fondasi *Decentralized Identifiers* (DIDs), *Verifiable Credentials* (VCs), dan digital *wallets* yang memungkinkan pengguna mengatur secara mandiri proses penerbitan,

penyimpanan, hingga pembagian identitas. Dengan mekanisme seperti *selective disclosure* dan *zero-knowledge proofs*, SSI mendukung prinsip *privasi-by-design*, di mana hanya data minimum yang diperlukan yang diungkapkan kepada pihak ketiga (Krul et al., 2024).

Peran *blockchain* dalam SSI dijelaskan lebih lanjut oleh Pava-Díaz et al., yang menekankan bahwa *ledger* berfungsi sebagai *trust anchor* untuk menyimpan dokumen DID, status kredensial, serta registrasi pencabutan. Data pribadi tetap berada di sisi pengguna, sementara *ledger* memastikan integritas dan keterverifikasian bukti identitas secara desentralisasi. Hal ini memperkuat penerapan prinsip *user control* dan data *minimization*, sekaligus mengurangi risiko sentralisasi yang rentan terhadap kebocoran (Pava-Díaz et al., 2024).

Implementasi nyata dari SSI di sektor kesehatan ditunjukkan oleh Harrell et al. [3], yang mengembangkan platform berbasis *Hyperledger Indy* guna mendukung manajemen identitas pasien. Dengan pendekatan ini, pasien memiliki kendali penuh atas akses kredensial medis mereka, sehingga privasi lebih terjaga sekaligus meningkatkan interoperabilitas antar lembaga layanan kesehatan. Hasil tersebut menunjukkan potensi SSI dalam memberikan kendali granular terhadap data sensitif sekaligus menjaga kepatuhan terhadap regulasi privasi (Harrell et al., 2022).

Selain itu, penelitian terbaru juga mengeksplorasi integrasi SSI dengan mekanisme kontrol akses berbasis *blockchain*. Sebuah studi pada *Journal of Network and Computer Applications* menunjukkan bahwa SSI dapat dikombinasikan dengan *zero-knowledge proofs* untuk mendukung privasi atribut dalam *sistem access control*, sehingga hanya informasi yang diperlukan yang terungkap tanpa membuka seluruh identitas pengguna (Di Francesco Maesa et al., 2023). Pendekatan ini relevan dengan prinsip *least privilege* dalam *Zero-Trust Architecture* (ZTA).

Di sisi lain, kerangka kerja multi-lapis untuk SSI berbasis *blockchain* juga telah dikembangkan. Penelitian ini mengusulkan *multi-layer trust framework* yang mendukung pengelolaan identitas, penerbitan kredensial, serta proses autentikasi dan verifikasi secara terdesentralisasi (De Salve et al., 2023). Dengan adanya lapisan kepercayaan berjenjang, SSI dapat lebih efektif dalam menjamin interoperabilitas lintas platform sekaligus menjaga kendali penuh pengguna atas data mereka.

Keunggulan Blockchain dalam Zero-Trust Architecture

Blockchain sebagai *ledger* terdistribusi yang bersifat *immutable* dan transparan memiliki potensi besar dalam memperkuat penerapan *Zero-Trust Architecture* (ZTA). Prinsip utama ZTA adalah *never trust, always verify*, yang menuntut mekanisme autentikasi, otorisasi, dan audit yang berkesinambungan. Dalam konteks ini, *blockchain* menghadirkan solusi desentralisasi untuk pengelolaan identitas digital melalui konsep *decentralized identifiers* (DID) dan *self-sovereign identity* (SSI), yang memungkinkan individu mengendalikan data pribadi sekaligus menyediakan bukti verifikasi berbasis kriptografi yang tidak dapat diubah (Bandara et al., 2021).

Manfaat utama integrasi *blockchain* pada ZTA adalah peningkatan keamanan identitas dengan mengurangi ketergantungan pada server otoritas pusat yang rentan menjadi target serangan. Melalui *blockchain*, verifikasi identitas dapat dilakukan dengan *zero-knowledge*

proofs atau *selective disclosure* tanpa harus membagikan seluruh data sensitif, sehingga sejalan dengan prinsip minimisasi kepercayaan dan *least-privilege access* (Pava-Díaz et al., 2024). Selain itu, *blockchain* juga memperkuat aspek auditabilitas dan non-repudiasi karena setiap transaksi dan status kredensial tersimpan dalam ledger yang transparan dan tidak dapat dimodifikasi (da Fonseca et al., 2023).

Selain itu, *smart contract* pada *blockchain* dapat digunakan untuk mengotomasi kebijakan akses dalam ZTA. Dengan mendefinisikan logika otorisasi yang dijalankan secara deterministik di *blockchain*, organisasi dapat memastikan bahwa keputusan akses bersifat konsisten, dapat diaudit, dan tidak tergantung pada satu otoritas tunggal (Nie et al., 2025). Penerapan ini memberikan nilai tambah berupa transparansi dan efisiensi, meskipun tetap menghadapi tantangan terkait performa, manajemen kunci, dan kepatuhan regulasi data pribadi.

Tantangan implementasi Blockchain dalam Zero-Trust Architecture

Integrasi *blockchain* ke dalam *Zero-Trust Architecture* (ZTA) menawarkan potensi untuk memperkuat manajemen identitas, meningkatkan auditabilitas, dan mengurangi ketergantungan pada penyedia identitas terpusat. Namun, upaya menggabungkan kedua konsep ini menghadirkan hambatan teknis, hukum, dan operasional yang signifikan.

Salah satu hambatan teknis paling mendasar adalah keterbatasan skalabilitas dan latensi pada banyak platform *blockchain* publik. ZTA menuntut verifikasi identitas dan keputusan akses secara cepat (*real-time*), sedangkan beberapa *blockchain* membatasi *throughput* transaksi per detik dan memiliki *latency* tinggi yang tidak cocok untuk operasi akses tingkat *enterprise* (Ghasemshirazi et al., 2023). Oleh karena itu, solusi murni *on-chain* untuk setiap elemen autentikasi sering tidak praktis, sehingga diperlukan pendekatan *hybrid* dengan *layer-2* atau *off-chain anchoring* (Mutahhar et al., 2025).

Imutabilitas *blockchain* berpotensi bertentangan dengan regulasi privasi seperti GDPR yang menuntut hak untuk dihapus (*right to be forgotten*). Menyimpan data pribadi secara *on-chain* dapat menimbulkan masalah hukum dan etika, sehingga perlu solusi *off-chain* dengan *hashing, zero-knowledge proofs*, atau *selective disclosure* (Godyn et al., 2022). Tantangan ini menjadikan integrasi *blockchain*-ZTA tidak hanya persoalan teknis, tetapi juga hukum dan regulasi lintas yurisdiksi. Keamanan *blockchain* bergantung pada *private key*, namun dalam konteks ZTA hal ini menimbulkan risiko kehilangan kunci, pencurian, atau kesalahan pengguna. Kompleksitas manajemen kunci pribadi mengurangi adopsi, sehingga dibutuhkan mekanisme pemulihan dan tata kelola kunci yang lebih praktis (Nikhil Ghadge, 2024). Hal ini semakin menantang ketika diintegrasikan dengan kebijakan *Zero-Trust* yang menuntut autentikasi berlapis dan kontrol *granular*.

KESIMPULAN

Penelitian ini menegaskan relevansi strategis integrasi teknologi *blockchain* dalam *Zero-Trust Architecture* (ZTA) untuk memperkuat keamanan identitas digital dan privasi data. Karakteristik unik *blockchain* yang desentralisasi, transparan, dan tidak dapat diubah menjadikannya fondasi penting bagi penerapan prinsip "*never trust, always verify*" dalam ZTA.

Melalui konsep *Decentralized Identifiers* (DID) dan *Self-Sovereign Identity* (SSI), *blockchain* tidak hanya memberikan kontrol penuh kepada pengguna atas data pribadinya, tetapi juga menghadirkan mekanisme autentikasi yang aman, minimasi pengungkapan informasi, serta auditabilitas yang dapat dipertanggungjawabkan. Meskipun demikian, integrasi *blockchain* dan ZTA masih menghadapi sejumlah kendala, mulai dari keterbatasan skalabilitas dan kompleksitas manajemen kunci, hingga tantangan kepatuhan hukum terhadap regulasi privasi global seperti GDPR. Oleh karena itu, diperlukan pendekatan *hybrid*, inovasi teknis berkelanjutan, serta kerangka regulasi yang adaptif untuk mengoptimalkan potensinya. Dengan demikian, *blockchain* dalam konteks ZTA bukan hanya sekadar teknologi pendukung, tetapi juga paradigma baru dalam tata kelola keamanan digital yang menuntut kolaborasi erat antara pemerintah, industri, dan akademisi guna mewujudkan sistem keamanan siber yang lebih andal dan berkelanjutan.

DAFTAR PUSTAKA

Allsop, D. B., Chelladurai, J. M., Kimball, E. R., Marks, L. D., & Hendricks, J. J. (2022). Qualitative Methods with Nvivo Software: A Practical Guide for Analyzing Qualitative Data. *Psych*, *4*(2), 142–159. https://doi.org/10.3390/psych4020013

Bandara, E., Liang, X., Foytik, P., Shetty, S., & Zoysa, K. De. (2021). A Blockchain and Self-Sovereign Identity Empowered Digital Identity Platform. *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, *2021-July*(January 2022). https://doi.org/10.1109/ICCCN52240.2021.9522184

Butincu, C. N., & Alexandrescu, A. (2024). Design Aspects of Decentralized Identifiers and Self-Sovereign Identity Systems. *IEEE Access*, *12*(February), 60928–60942. https://doi.org/10.1109/ACCESS.2024.3394537

Carcary, M. (2020). The Research Audit Trail: Methodological Guidance for Application in Practice. *Electronic Journal of Business Research Methods*, *18*(2), 166–177. https://doi.org/10.34190/JBRM.18.2.008

Chaudhry, U. B., & Hydros, A. K. M. (2023). Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm. *IET Blockchain*, *3*(2), 98–115. https://doi.org/10.1049/blc2.12028

Choe, Y., Lee, J., & Lee, G. (2022). Exploring Values via the Innovative Application of Social Media with Parks Amid COVID-19: A Qualitative Content Analysis of Text and Images Using ATLAS.ti. *Sustainability (Switzerland)*, *14*(20). https://doi.org/10.3390/su142013026

da Fonseca, L. M. M., Barzegar, H. R., & Pahl, C. (2023). Decentralized Identification and Information Exchange in Distributed, Blockchain-Based Internet Architectures: A Technology Review. *International Conference on Web Information Systems and*

Technologies, WEBIST - Proceedings, *Webist*, 535–544. https://doi.org/10.5220/0012254900003584

De Salve, A., Di Francesco Maesa, D., Mori, P., Ricci, L., & Puccia, A. (2023). A multi-layer trust framework for Self Sovereign Identity on blockchain. *Online Social Networks and Media*, *37–38*(February), 100265. https://doi.org/10.1016/j.osnem.2023.100265

Di Francesco Maesa, D., Lisi, A., Mori, P., Ricci, L., & Boschi, G. (2023). Self sovereign and blockchain based access control: Supporting attributes privacy with zero knowledge. *Journal of Network and Computer Applications*, *212*(July 2022), 103577. https://doi.org/10.1016/j.jnca.2022.103577

Enaya, A., Fernando, X., & Kashef, R. (2025). Survey of Blockchain-Based Applications for IoT. *Applied Sciences (Switzerland)*, *15*(8). https://doi.org/10.3390/app15084562

Garzon, S. R., Segat, C., & Kupper, A. (2025). Governance of Ledger-Anchored Decentralized Identifiers. *Proceedings - 2025 Crypto Valley Conference, CVC 2025*, 44–55. https://doi.org/10.1109/CVC65719.2025.00014

Ghasemshirazi, S., Shirvani, G., & Alipour, M. A. (2023). *Zero Trust: Applications, Challenges, and Opportunities*.

Godyn, M., Kedziora, M., Ren, Y., Liu, Y., & Song, H. H. (2022). Analysis of solutions for a blockchain compliance with GDPR. *Scientific Reports*, *12*(1), 1–11. https://doi.org/10.1038/s41598-022-19341-y

Harrell, D. T., Usman, M., Hanson, L., Abdul-Moheeth, M., Desai, I., Shriram, J., de Oliveira, E., Bautista, J. R., Meyer, E. T., & Khurshid, A. (2022). Technical Design and Development of a Self-Sovereign Identity Management Platform for Patient-Centric Health Care using Blockchain Technology. *Blockchain in Healthcare Today*, *5*(Special issue), 1–12. https://doi.org/10.30953/bhty.v5.196

Horne, D. (2025). Zero Trust Architecture. *Encyclopedia of Cryptography, Security and Privacy, Third Edition*, 2809–2814. https://doi.org/10.1007/978-3-030-71522-9_1638

Kim, G., & Ryou, J. (2023). Digital Authentication System in Avatar Using DID and SBT. *Mathematics*, *11*(20). https://doi.org/10.3390/math11204387

Kriswandaru, A. S., Pratiwi, B., Laksito, J., Ariani, W., & Sholikatun, S. (2025). Analisis Yuridis terhadap Penggunaan Teknologi Blockchain dalam Pengamanan Data Pribadi: Studi Kasus di Indonesia. *Perkara : Jurnal Ilmu Hukum Dan Politik*, *2*(4), 531–540. https://doi.org/10.51903/perkara.v2i4.2225

Krul, E., Paik, H., Ruj, S., & Kanhere, S. S. (2024). SoK: Trusting Self-Sovereign Identity. In *Proceedings on Privacy Enhancing Technologies* (Vol. 2024, Issue 3). Association for Computing Machinery. https://doi.org/10.56553/popets-2024-0079

Mandinyenya, G., & Malele, V. (2025). A Hybrid Framework for Enhancing Privacy in Blockchain-Based Personal Data Sharing using Off-Chain Storage and Zero-Knowledge Proofs. *Journal of Information Systems and Informatics*, *7*(2), 1977–2005. https://doi.org/10.51519/journalisi.v7i2.1119

Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., & Conti, M. (2025). A Survey on Decentralized Identifiers and Verifiable Credentials. *IEEE Communications Surveys and Tutorials*, 1–32. https://doi.org/10.1109/COMST.2025.3543197

Mutahhar, A., Khanzada, T. J. S., & Shahid, M. F. (2025). Enhanced Scalability and Security in Blockchain-Based Transportation Systems for Mass Gatherings. *Information*, *16*(8), 641. https://doi.org/10.3390/info16080641

Nie, S., Ren, J., Wu, R., Han, P., Han, Z., & Wan, W. (2025). Zero-Trust Access Control Mechanism Based on Blockchain and Inner-Product Encryption in the Internet of Things in a 6G Environment. *Sensors*, *25*(2), 1–27. https://doi.org/10.3390/s25020550

Nikhil Ghadge. (2024). Analyzing the Role of Blockchain in Identity and Access Management Systems. *International Journal of Science and Research Archive*, *12*(1), 2249–2256. https://doi.org/10.30574/ijsra.2024.12.1.1019

Pava-Díaz, R. A., Gil-Ruiz, J., & López-Sarmiento, D. A. (2024). Self-sovereign identity on the blockchain: Contextual analysis and quantification of SSI principles implementation. *Frontiers in Blockchain*, *7*(August), 1–15. https://doi.org/10.3389/fbloc.2024.1443362

Polychronaki, M., Xevgenis, M. G., Kogias, D. G., & Leligou, H. C. (2024). Decentralized Identity Management for Metaverse-Enhanced Education: A Literature Review. *Electronics (Switzerland)*, *13*(19). https://doi.org/10.3390/electronics13193887

Schumm, D., Muller, K. O. E., & Stiller, B. (2025). Are We There Yet? A Study of Decentralized Identity Applications. *IEEE Access*, *13*, 125232–125259. https://doi.org/10.1109/ACCESS.2025.3588170

Singh, A., Pareek, V., & Sharma, A. (2024). A Review on Blockchain for Fintech using Zero Trust Architecture. *Journal of Information and Organizational Sciences*, *48*(1), 191–213. https://doi.org/10.31341/jios.48.1.11

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. https://doi.org/10.21787/jskp.2.2023.55-68

Wang, F., Gai, Y., & Zhang, H. (2024). Blockchain user digital identity big data and information security process protection based on network trust. *Journal of King Saud University - Computer and Information Sciences*, *36*(4), 102031. https://doi.org/10.1016/j.jksuci.2024.102031

Wendelborn, C., Anger, M., & Schickhardt, C. (2023). What is data stewardship? Towards a comprehensive understanding. *Journal of Biomedical Informatics*, *140*(March), 104337. https://doi.org/10.1016/j.jbi.2023.104337

Xie, T., Gai, K., Yu, J., Zhu, L., & Xiao, B. (2025). *SLVC-DIDA: Signature-less Verifiable Credential-based Issuer-hiding and Multi-party Authentication for Decentralized Identity*. *Did*.