**JRIIN : Jurnal Riset Informatika dan Inovasi**
**Volume 3, No. 10 Maret Tahun 2026**
**ISSN 3025-0919 (media online)**
**Hal 2605-2611**

# Pemanfaatan Teknologi Blockchain dalam Menangkal Ancaman Keamanan Siber pada Sistem Informasi

**Muhamad Tegar Surya Permana[1], Saripudin[2]**

[1,2] Fakultas Ilmu Komputer, Program Studi Sistem Informasi, Universitas Pamulang, Tangerang Selatan, Indonesia
Email: [1]muhamadtegarsp27@gmail.com, [2]saripudin2249@gmail.com

**Abstrak**−Perkembangan sistem informasi saat ini mendorong organisasi untuk semakin bergantung pada teknologi digital dalam mendukung aktivitas operasional. Namun, kondisi tersebut turut meningkatkan risiko ancaman keamanan siber, seperti kebocoran data, manipulasi informasi, dan gangguan layanan sistem. Arsitektur sistem informasi yang masih bersifat terpusat dinilai memiliki tingkat kerentanan yang tinggi terhadap berbagai bentuk serangan siber. Oleh karena itu, teknologi blockchain mulai dipertimbangkan sebagai alternatif solusi keamanan karena karakteristik desentralisasi dan ketidakterubahan data yang dimilikinya. Penelitian ini bertujuan untuk mengkaji pemanfaatan teknologi blockchain dalam menangkal ancaman keamanan siber pada sistem informasi melalui pendekatan kualitatif berbasis studi literatur. Sumber data diperoleh dari jurnal ilmiah, buku, dan whitepaper yang relevan. Hasil kajian menunjukkan bahwa penerapan karakteristik blockchain, seperti desentralisasi, transparansi, dan immutability, berpotensi memperkuat aspek keamanan data serta integritas sistem informasi. Penelitian ini diharapkan dapat menjadi rujukan awal bagi pengembangan sistem informasi yang lebih aman.

**Kata Kunci:** ; Blockchain; Keamanan Siber; Sistem Informasi; Keamanan Data

**Abstract**−*The current development of information systems encourages organizations to increasingly rely on digital technologies to support operational activities. However, this condition also increases the risk of cybersecurity threats, such as data breaches, information manipulation, and system service disruptions. Information system architectures that are still centralized are considered to have a high level of vulnerability to various forms of cyberattacks. Therefore, blockchain technology has begun to be considered as an alternative security solution due to its characteristics of decentralization and data immutability. This study aims to examine the utilization of blockchain technology in countering cybersecurity threats in information systems through a qualitative approach based on a literature study. Data sources were obtained from relevant scientific journals, books, and whitepapers. The results of the study indicate that the implementation of blockchain characteristics, such as decentralization, transparency, and immutability, has the potential to enhance data security and the integrity of information systems. This study is expected to serve as an initial reference for the development of more secure information systems.*

**Keywords**: *; Blockchain; Cybersecurity; Information Systems; Data Security*

## 1. PENDAHULUAN

Integrasi teknologi informasi ke dalam seluruh aspek operasional organisasi telah membawa perubahan fundamental terhadap efisiensi kerja secara global. Digitalisasi saat ini bukan lagi sekadar pilihan strategis, melainkan kebutuhan infrastruktur utama untuk menjaga keberlangsungan sistem informasi di era industri 4.0. Namun, di balik kemudahan aksesibilitas tersebut, muncul risiko signifikan berupa kerentanan terhadap serangan siber yang kian kompleks. Oleh karena itu, keamanan sistem informasi sebagai upaya perlindungan aset informasi dari ancaman demi memastikan keberlangsungan bisnis, meminimalkan risiko, serta memaksimalkan investasi dan peluang bisnis menjadi sangat krusial (Jupron S.Kom. et al., 2025). Fenomena kejahatan siber (*cybercrime*) seperti kebocoran data (*data breach)*, serangan *malware*, hingga manipulasi informasi menjadi tantangan serius yang mengancam integritas data pada sistem informasi yang masih bergantung pada arsitektur basis data terpusat.

Masalah utama yang sering menjadi titik lemah adalah ketergantungan pada satu otoritas kontrol tunggal atau *Single Point of Failure* (SPOF). Menurut laporan literatur terbaru dari (Prakash et al., 2022), ancaman seperti *Denial of Service* (DoS) bukan hanya sekadar gangguan teknis operasional, melainkan ancaman utama yang dapat melumpuhkan ketersediaan informasi dalam skala masif. Statistik menunjukkan bahwa sistem keamanan konvensional mulai mencapai batas optimalnya dalam menghadapi eksploitasi kerentanan yang frekuensinya terus meningkat secara eksponensial dalam sepuluh tahun terakhir.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 10 Maret Tahun 2026
ISSN 3025-0919 (media online)
Hal 2605-2611

Dalam situasi krisis keamanan pada sistem terpusat inilah, teknologi hadir menawarkan paradigma baru. Sejarah mencatat bahwa kemunculan teknologi ini berakar dari konsep desentralisasi yang diperkenalkan oleh Satoshi Nakamoto dalam *whitepaper* fundamentalnya pada tahun 2008. Nakamoto memperkenalkan sistem transaksi yang tidak memerlukan verifikasi dari pihak ketiga yang tepercaya (*trusted third party*), melainkan mengalihkan mekanisme validasi kepada algoritma kriptografi yang transparan (Nakamoto, 2008) bekerja dengan mendistribusikan data ke seluruh jaringan *peer-to-peer*, sehingga setiap blok informasi yang saling terikat secara kronologis menjadi hampir mustahil untuk dimodifikasi tanpa adanya persetujuan mayoritas dari node jaringan.

Pemanfaatan dalam sistem informasi tidak hanya menjanjikan ketidakterubahan data (*immutability*), tetapi juga membangun struktur pertahanan yang terdesentralisasi. Melalui mekanisme konsensus dan keamanan berlapis, risiko manipulasi data dapat diminimalisir karena setiap jejak transaksi terekam secara permanen dan memiliki sifat auditabel oleh seluruh partisipan dalam jaringan (Moosavi & Taherdoost, 2023).

Di Indonesia sendiri, urgensi penguatan keamanan siber menjadi prioritas nasional seiring dengan meningkatnya frekuensi insiden kebocoran data pada berbagai institusi publik maupun swasta. Upaya pencarian solusi alternatif selain sistem konvensional mulai mengarah pada adopsi teknologi mutakhir. Sejalan dengan hal tersebut, penelitian oleh (Widiyati & Erliana, 2024) menegaskan bahwa pemanfaatan teknologi di Indonesia memiliki potensi besar dalam mentransformasi standar keamanan data pada sistem informasi nasional. Implementasi dinilai mampu memberikan lapisan perlindungan ekstra melalui mekanisme enkripsi yang lebih tangguh, sehingga risiko manipulasi informasi oleh pihak yang tidak bertanggung jawab dapat ditekan secara signifikan dalam ekosistem digital Indonesia.

Berdasarkan fenomena kerentanan pada sistem keamanan tradisional tersebut, penelitian ini bertujuan untuk menganalisis pemanfaatan teknologi *blockchain* sebagai instrumen strategis dalam menangkal ancaman keamanan siber pada sistem informasi. Melalui kajian kualitatif dengan pendekatan studi literatur ini, diharapkan dapat dirumuskan sebuah kerangka keamanan yang lebih tangguh, transparan, dan adaptif terhadap dinamika serangan siber di masa depan.

## 2. METODE PENELITIAN

### 2.1 Rancangan dan Pendekatan Penelitian

Dalam upaya membedah potensi teknologi secara mendalam, penelitian ini mengadopsi metode kualitatif dengan kerangka studi literatur. Pemilihan pendekatan ini didasarkan pada kebutuhan untuk mengevaluasi beragam teori, temuan empiris, serta dokumentasi teknis yang telah ada sebelumnya. Penulis memposisikan diri sebagai pengkaji yang melakukan sintesis terhadap berbagai sumber pustaka guna membangun pemahaman komprehensif mengenai bagaimana arsitektur desentralisasi dapat menjawab kelemahan sistem keamanan informasi tradisional.

### 2.2 Teknik Pengumpulan dan Analisis Data

Proses pengumpulan data dilakukan melalui penelusuran sistematis pada berbagai pangkalan data ilmiah digital yang kredibel, termasuk *ScienceDirect*, Google Scholar, dan beberapa portal jurnal nasional terakreditasi. Penulis menggunakan kombinasi kata kunci yang spesifik seperti "", "Integritas Data", serta "Keamanan Siber" untuk menjaring literatur yang relevan.

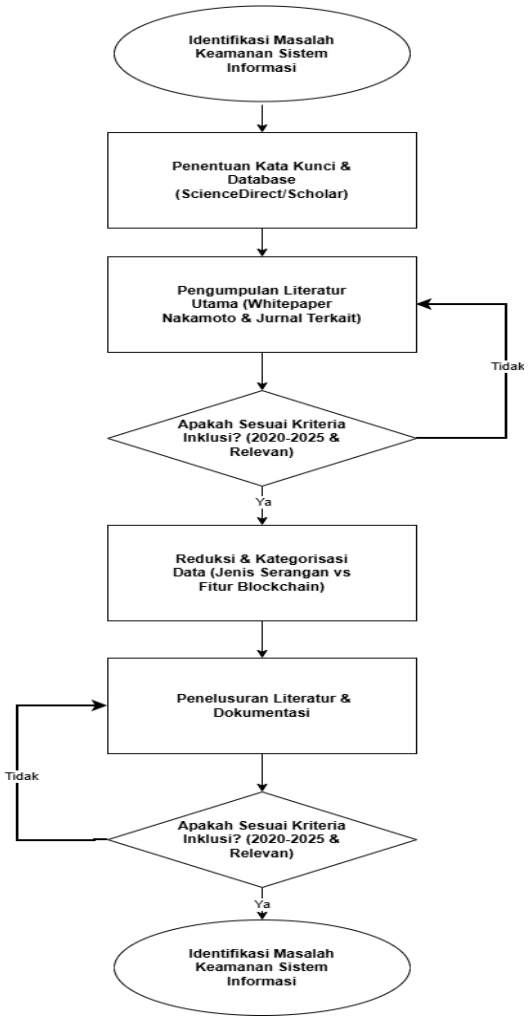
Guna menjamin validitas dan kebaruan informasi, penulis menetapkan batasan ketat dalam pemilihan sumber, yakni hanya menggunakan jurnal yang diterbitkan dalam rentang tahun 2020 hingga 2025. Namun, pengecualian diberikan pada dokumen fundamental seperti *whitepaper Bitcoin* karya (Nakamoto, 2008) yang dianggap sebagai referensi primer wajib dalam memahami akar teknologi ini. Adapun kriteria inklusi dan parameter penelusuran yang digunakan dirangkum dalam tabel berikut:

**Tabel 1.** Parameter Penelusuran

| Parameter | Kriteria Inklusi (Diterima) | Kriteria Eksklusi (Ditolak) |
|---|---|---|
| Rentang Waktu | Tahun 2020 – 2025 (Kecuali sumber primer Nakamoto 2008). | Literatur yang terbit di bawah tahun 2020. |

**JRIIN : Jurnal Riset Informatika dan Inovasi**
**Volume 3, No. 10 Maret Tahun 2026**
**ISSN 3025-0919 (media online)**
**Hal 2605-2611**

| | | |
|---|---|---|
| Jenis Sumber | Jurnal Ilmiah (SINTA/Scopus), *Conference Paper*, dan *Whitepaper* teknis. | Blog pribadi, berita populer, atau artikel tanpa identitas penulis. |
| Bahasa | Bahasa Indonesia dan Bahasa Inggris. | Selain bahasa Indonesia dan Inggris. |
| Kata Kunci (*Keywords*) | *Cybersecurity, Data Integrity, Decentralization, Smart Contracts.* | Teknologi database terpusat yang tidak relevan dengan keamanan siber. |
| Fokus Bahasan | Mekanisme teknis dalam memitigasi serangan siber. | Pembahasan yang hanya fokus pada nilai investasi/kripto. |




**Gambar 1.** Flowchart alur Pengambilan Data

### 2.3 Prosedur Analisis Data

Setelah data terkumpul, tahap selanjutnya adalah melakukan analisis deskriptif-analitis. Penulis mengadopsi pola pemetaan tema sebagaimana yang diterapkan oleh (Prakash et al., 2022) dalam mengidentifikasi korelasi antara kerentanan sistem dengan solusi teknologi yang ditawarkan. Analisis dilakukan dengan cara membandingkan secara kritis keterbatasan sistem database terpusat (seperti kerentanan terhadap manipulasi admin) dengan mekanisme keamanan yang melekat pada *blockchain* (seperti hashing dan konsensus). Seluruh referensi yang dikutip dalam artikel ini disusun

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 10 Maret Tahun 2026
ISSN 3025-0919 (media online)
Hal 2605-2611

dengan mengikuti kaidah penulisan ilmiah yang berlaku untuk menjaga integritas dan transparansi akademik.

## 3. ANALISA DAN PEMBAHASAN

Seiring dengan meningkatnya kompleksitas serangan siber yang mengancam integritas dan kerahasiaan data, diperlukan evaluasi terhadap solusi keamanan yang lebih tangguh. Bab ini akan menganalisis bagaimana mekanisme desentralisasi dan imutabilitas pada teknologi *blockchain* dapat merespons berbagai ancaman modern, sekaligus mengidentifikasi batasan-batasan implementasinya dalam sistem informasi saat ini.

### 3.1 Ancaman Keamanan Siber pada Sistem Informasi

Sistem informasi di era digital terkini menghadapi lanskap ancaman keamanan siber yang semakin kompleks dan canggih. Ancaman tradisional seperti *data breach*, serangan *malware* termasuk varian *ransomware* yang semakin terarah dengan tuntutan tebusan aset kripto serta penyalahgunaan akses oleh pihak internal (*insider threat*) tetap menjadi tantangan besar bagi integritas data.

Namun, perkembangan teknologi juga melahirkan vektor serangan baru yang lebih masif, seperti eksploitasi kerentanan pada perangkat *Internet of Things* (IoT), serangan pada rantai pasok (*supply-chain*) yang menargetkan pihak ketiga, serta pemanfaatan *deepfake* untuk aktivitas rekayasa sosial (*social engineering*). Industrialisasi kejahatan siber melalui model *Ransomware-as-a-Service* (RaaS) juga mempermudah pelaku dengan kapabilitas teknis rendah untuk melakukan serangan berskala besar.

Ancaman-ancaman ini tidak hanya mengganggu elemen integritas, kerahasiaan, dan ketersediaan (*Triad CIA*) pada data, tetapi juga berpotensi melumpuhkan operasional kritis serta menimbulkan kerugian finansial yang signifikan. Sejalan dengan fenomena ini, (Widiyati & Erliana, 2024) menegaskan bahwa meningkatnya frekuensi insiden kebocoran data di berbagai institusi menuntut adanya penguatan mekanisme perlindungan informasi melalui teknologi yang lebih tangguh. Kerentanan utama pada sistem konvensional umumnya terletak pada ketergantungan kontrol otoritas tunggal yang menciptakan *Single Point of Failure* (SPOF).

Sebagai rincian dari klasifikasi ancaman yang telah dijelaskan, berikut adalah tabel rangkuman jenis serangan beserta dampaknya terhadap infrastruktur informasi:

**Tabel 2.** Klasifikasi Ancaman Siber dan Dampaknya

| Kategori Ancaman | Jenis Serangan Utama | Dampak Pada Sistem Informasi |
|---|---|---|
| Ketersedian | DDoS, DoS, *Ransomware* | Terhentinya layanan operasional akibat hilangnya akses ke pusat data. |
| Integritas | Manipulasi Data, *Injeksi Malware* | Perubahan data secara ilegal yang merusak keakuratan informasi. |
| Kerahasiaan | *Data Breach, Phishing, Deepfake* | Paparan data sensitif kepada pihak yang tidak memiliki hak akses. |

### 3.2 Mekanisme Keamanan Teknologi Blockchain

Teknologi *blockchain* menyediakan lapisan keamanan yang fundamental melalui arsitektur yang berbeda dari sistem basis data tradisional. Terdapat beberapa mekanisme inti yang memungkinkan menjadi instrumen pertahanan siber yang tangguh menurut (Moosavi & Taherdoost, 2023):

a. Desentralisasi dan Buku Besar Terdistribusi (*Distributed Ledger*) Berbeda dengan sistem terpusat, *blockchain* mendistribusikan salinan data ke seluruh node dalam jaringan. Sesuai dengan konsep yang diperkenalkan (Nakamoto, 2008), hal ini menghilangkan *Single Point of Failure* (SPOF), sehingga penyerang tidak dapat melumpuhkan sistem hanya dengan menyerang satu titik server pusat.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 10 Maret Tahun 2026
ISSN 3025-0919 (media online)
Hal 2605-2611

b. Fungsi *Hash* Kriptografi Setiap blok informasi dihubungkan menggunakan sidik jari digital unik yang disebut hash. Jika terjadi perubahan data sekecil apa pun pada satu blok, maka nilai hash tersebut akan berubah dan memutus rantai hubungan dengan blok berikutnya. Mekanisme ini menjamin integritas data tetap terjaga.
c. Mekanisme Konsensus Keamanan *blockchain* bergantung pada algoritma konsensus, di mana mayoritas partisipan jaringan harus memvalidasi setiap transaksi sebelum dicatat secara permanen. Hal ini mencegah pihak tidak bertanggung jawab untuk memasukkan data palsu ke dalam buku besar.
d. Imutabilitas dan Jejak Audit Sifat *immutability* memastikan data yang telah mencapai konsensus tidak dapat dihapus atau dimodifikasi kembali, sehingga menciptakan jejak audit yang transparan. Implementasi keamanan ini juga berkaitan dengan efisiensi pengelolaan protokol penyimpanan data kriptografi yang terstruktur, sebagaimana dijelaskan dalam penelitian (Hafizh Fianto Putra, 2022).

Untuk mempermudah pemahaman mengenai perbedaan mekanisme keamanan ini, Tabel 3 menyajikan perbandingan antara sistem konvensional dan teknologi *blockchain*:

**Tabel 3.** Perbandingan Keamanan Sistem Terpusat vs *Blockchain*

| Aspek Keamanan | Sistem Terpusat (Konvensional) | Teknologi |
|---|---|---|
| Arsitektur | Otoritas Tunggal (SPOF). | Jaringan Terdistribusi |
| Penyimpanan Data. | Dapat diubah oleh admin/hacker. | *Immutability* (Permanen). |
| Verifikasi. | Verifikasi Pihak Ketiga. | Konsensus Jaringan (*Peer-to-Peer*). |
| Transparansi. | Terbatas (*Closed System*). | Transparan dan Dapat diaudit. |

### 3.3 Analisis Peran Blockchain dalam Menangkal Ancaman Keamanan Siber

Teknologi *blockchain* menjalankan peran strategis dalam memitigasi risiko siber yang telah dipaparkan sebelumnya. Berikut adalah analisis bagaimana *blockchain* merespons ancaman tersebut:

a. Proteksi integritas data melalui sifat *immutability*, menjamin bahwa informasi yang telah tersimpan tidak dapat dimodifikasi tanpa persetujuan jaringan. Hal ini secara efektif menangkal upaya manipulasi data dan serangan *ransomware*, karena sistem akan menolak setiap data yang tidak sinkron dengan catatan pada blok sebelumnya.
b. Mitigasi risiko kelumpuhan sistem (ddos) struktur jaringan yang terdistribusi meniadakan ketergantungan pada satu server tunggal. Dampaknya, serangan *Denial of Service* (dos) sulit untuk melumpuhkan layanan secara total, mengingat operasional sistem tetap terjaga oleh node lain yang tersebar di dalam jaringan.
c. Auditabilitas dan transparansi transaksi setiap aktivitas dalam buku besar meninggalkan jejak digital yang permanen. Hal ini memudahkan proses audit dan deteksi dini terhadap upaya kebocoran data (*data breach*), karena setiap pergerakan informasi dapat divalidasi secara transparan oleh pihak berwenang.
d. Penguatan autentikasi pengguna penggunaan kriptografi kunci publik-privat pada memberikan proteksi lebih tinggi pada identitas digital. Mekanisme ini memperkecil peluang keberhasilan serangan rekayasa sosial (*social engineering*) atau pencurian akun yang sering menyasar kelemahan pada sistem kata sandi konvensional.

Penjelasan di atas menunjukkan bagaimana merespons berbagai jenis serangan siber. Secara lebih ringkas, kaitan antara ancaman siber dan solusi teknis yang ditawarkan dapat dilihat pada tabel berikut:

**Tabel 4.** Matriks Solusi *Blockchain* terhadap Ancaman Keamanan Siber

| Jenis Ancaman | Mekanisme Solusi | Peran Strategis |
|---|---|---|
| *Ransomware* Manipulasi | *Immutability* & *Hashing* | Mencegah perubahan data ilegal secara permanen. |

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 3, No. 10 Maret Tahun 2026
ISSN 3025-0919 (media online)
Hal 2605-2611

| | | |
|---|---|---|
| Serangan DdoS | Arsitektur Desentralisasi | Menghilangkan titik pusat serangan *(No SPOF).* |
| *Data Breach* | Kriptografi Kunci Publik | Mengamankan akses dan identitas pengguna. |
| *Insider Threat* | Mekanisme Konsensus | Memerlukan persetujuan mayoritas untuk validasi data. |

### 3.4 Kelebihan dan Keterbatasan Blockchain

Kelebihan utama *blockchain* untuk keamanan siber terletak pada desentralisasi, transparansi, kekekalan, dan ketahanannya. Prinsip-prinsip ini secara intrinsik mengurangi risiko manipulasi, penipuan, dan gangguan layanan terpusat. juga memungkinkan automasi keamanan melalui kontrak pintar (*smart contracts*), yang dapat mengeksekusi perjanjian atau prosedur keamanan secara otomatis dan tanpa perantara ketika kondisi terpenuhi. Namun, memiliki keterbatasan signifikan yang perlu dipertimbangkan secara teknis.

Skalabilitas dan Latensi: Proses konsensus sering kali lambat dan mahal energi, sehingga membatasi *throughput* transaksi terutama untuk kebutuhan aplikasi *real-time* (Jain et al., 2025). Privasi: Transparansi publik pada terbuka bisa menjadi bumerang untuk data sensitif, meskipun *blockchain* izinan (*permissioned*) dan teknik *zero-knowledge proof* sedang dikembangkan untuk mengatasinya. Manajemen Kunci: Keamanan bergantung sepenuhnya pada penyimpanan kunci privat pengguna; jika kunci hilang atau dicuri, aset dan akses tidak dapat dipulihkan. Keterbatasan *Scope*: Seperti dianalisis sebelumnya, tidak mengamankan sistem di luar rantainya (*off-chain*).

Kepatuhan Hukum dan Tata Kelola: Status hukum data yang *immutable* dapat bertentangan dengan regulasi seperti *Right to be Forgotten* dalam undang-undang perlindungan data pribadi (Sidi et al., 2025). Oleh karena itu, adopsi harus dipertimbangkan secara strategis sebagai bagian dari arsitektur keamanan berlapis, bukan sebagai pengganti seluruh mekanisme keamanan tradisional. Keberhasilan implementasi ini pada akhirnya tetap bergantung pada kesiapan literasi pengguna dalam memahami dasar-dasar keamanan siber dan kriptografi di tingkat operasional (Agus Budi Prasetyo1 et al., 2024). Dibawah ini adalah ringkasan mengenai kelebihan dan keterbatasan implementasi *blockchain* dalam sistem keamanan informasi:

**Tabel 5.** Analisis Kelebihan dan Keterbatasan Teknologi *Blockchain*

| Aspek | Kelebihan (*Advantages*) | Keterbatasan (*Limitations*) |
|---|---|---|
| Keamanan Data | *Immutability* mencegah manipulasi data secara ilegal. | Ketergantungan penuh pada keamanan kunci privat (*Private Key*). |
| Arsitektur | Desentralisasi menghilangkan risiko *Single Point of Failure*. | Konsumsi energi tinggi dan latensi pada proses konsensus. |
| Transparansi | Jejak audit yang terbuka dan mudah diverifikasi. | Potensi paparan data sensitif pada jaringan *blockchain* publik.. |
| Regulasi | Automasi keamanan melalui *Smart Contracts*. | Tantangan kepatuhan terhadap hak penghapusan data (UU PDP). |

## 4. KESIMPULAN

Berdasarkan hasil analisis terhadap karakteristik teknologi serta relevansinya dalam memperkuat keamanan siber, penelitian ini menyimpulkan bahwa sifat fundamental *desentralisasi*, transparansi, dan i*mmutability* merupakan fondasi utama bagi keamanan digital masa depan. Penelitian ini menemukan bahwa dengan meniadakan otoritas tunggal, risiko manipulasi data dan peretasan dapat ditekan secara signifikan karena struktur kriptografis antarblok secara otomatis menjaga integritas informasi. Hal ini membuktikan bahwa bukan sekadar tempat penyimpanan data, melainkan instrumen perlindungan aktif yang sangat efektif untuk mengamankan transaksi digital.

Penelitian ini juga menegaskan peran strategis dalam memitigasi *cybercrime* melalui mekanisme konsensus kolektif dan enkripsi terdistribusi. Verifikasi otomatis oleh node-node independen serta penggunaan *smart contract* terbukti mampu meminimalisasi keterlibatan pihak

ketiga yang sering kali menjadi titik lemah dalam serangan rekayasa sosial maupun pelanggaran data. Temuan ini mengarahkan pada kesimpulan bahwa adalah solusi yang sangat dapat dipercaya untuk membangun ekosistem transaksi yang aman dan transparan di masyarakat luas.

Sebagai rekomendasi akhir, penelitian ini menekankan perlunya strategi kolaboratif antara pemerintah, industri, dan akademisi di Indonesia. Diperlukan kerangka regulasi yang lebih adaptif untuk mengakomodasi teknologi desentralisasi ini tanpa mematikan inovasi nasional. Peningkatan literasi digital dan investasi pada riset akademik menjadi persyaratan mutlak agar potensi tidak hanya berhenti pada tataran teori, tetapi dapat menjadi pilar utama sistem keamanan digital nasional yang tangguh dan berdaya saing global.

## REFERENCES

Agus Budi Prasetyo, A.B., Tio Andrian, & Khoirunnisya. (2024). *PELATIHAN KRIPTOGRAFI DASAR DAN EDUKASI KEAMANAN SIBER DI SMK PUSPITA BANGSA CIPUTAT*.

Hafizh Fianto Putra, W. dan O. P. F. P. W. dan O. P. (2022). *Penerapan Blockchain dan Kriptografi untuk Keamanan Data pada Jaringan Smart Grid*.

Jain, A. K., Gupta, N., & Gupta, B. B. (2025). A survey on scalable consensus algorithms for blockchain technology. *Cyber Security and Applications*, *3*. https://doi.org/10.1016/j.csa.2024.100065

Jupron S.Kom., M. K., Emi Sita Eriana S.Kom., M. K., & Nanang S.Kom., M. K. (2025). *keamanan sistem dan infrastruktur jaringan*.

Moosavi, N., & Taherdoost, H. (2023). Blockchain Technology Application in Security: A Systematic Review. *Blockchains*, *1*(2), 58–72. https://doi.org/10.3390/blockchains1020005

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org

Prakash, R., Anoop, V. S., & Asharaf, S. (2022). Blockchain technology for cybersecurity: A text mining literature analysis. In *International Journal of Information Management Data Insights* (Vol. 2, Issue 2). Elsevier B.V. https://doi.org/10.1016/j.jjimei.2022.100112

Sidi, I., Wiraguna, A., Ars, M., & Barthos, M. (2025). *HUKUM PRIVASI DAN PELINDUNGAN DATA PRIBADI DI INDONESIA*. www.freepik.com

Widiyati, D., & Erliana. (2024). PENGARUH LITERASI KEUANGAN, PERLINDUNGAN DATA, DAN CYBERSECURITY TERHADAP PENGGUNAAN FINANCIAL TECHNOLOGY. *JAE (JURNAL AKUNTANSI DAN EKONOMI)*, *9*(1), 130–141. https://doi.org/10.29407/jae.v9i1.21945