

Analisis Implementasi Keamanan Data melalui Teknologi Blockchain

Muhammad Ali Anhar¹, Teguh Agum Pratama²

¹Program Studi Ilmu Komputer, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara, Jl. Lap. Golf No.120, Kp. Tengah, Kec. Pancur Batu, Kabupaten Deli Serdang, Sumatera Utara 20353

²Program Studi Ilmu Komunikasi, Fakultas Ilmu Sosial, Universitas Islam Negeri Sumatera Utara, Jl. Lap. Golf No.120, Kp. Tengah, Kec. Pancur Batu, Kabupaten Deli Serdang, Sumatera Utara 20353

Email: alianhar30704@gmail.com, teguh0603202104@uinsu.ac.id

Corresponding: teguh0603202104@uinsu.ac.id

Submitted:16-04-2024; Accepted: 20-05-2024; Published: 06-06-2024

ABSTRACT

This article examines the implementation of blockchain as a protective data feature at Pustipada UINSU. It focuses on the use of blockchain to maintain the data integrity of the academic community at the Universitas Islam Negeri Sumatera Utara campus. Thus, blockchain has the potential to protect data from hacking or leakage activities. However, blockchain implementation faces several challenges, such as overly centralized network integrity, high implementation costs and complexity, cultural change, necessary understanding, and support from relevant parties. Data security, especially user privacy, is also a concern due to the public nature of the blockchain ledger. A careful strategy is needed to enhance privacy without compromising the security advantages offered by blockchain. This study uses a qualitative descriptive method and a case study approach. It analyzes the comprehensive implementation of blockchain technology in data security at Pustipada UINSU. The study utilizes cryptography theory to support research arguments. Data collection techniques include interviews, direct observations, and document analysis. Data analysis considers technical, social, and infrastructural factors influencing implementation success. Blockchain technology, based on cryptography, offers significant prospects for adoption in various sectors, including education. In the specific context of the university's database or Pustipada UINSU, implementing blockchain technology can significantly enhance data protection and integrity. Several critical aspects need to be considered. a) Existing information technology infrastructure must support blockchain implementation. b) Compliance with applicable laws and regulations must also be considered. c) Adequate understanding of blockchain technology among users and stakeholders is crucial.

Keywords: Blockchain, Cryptography, Data Security, Pustipada UINSU.

ABSTRAK

Artikel ini mengkaji terkait penerapan blockchain sebagai fitur protektif data di Pustipada UINSU. Hal ini, menjadi fokus kajian terhadap pemanfaatan blockchain untuk menjaga integritas data civitas akademik kampus Universitas Islam Negeri Sumatera Utara. Sehingga, blockchain memiliki potensial dalam penjagaan kewanitaan data untuk menghindari aktivitas peretasan maupun kebocoran data. Namun, Implementasi blockchain dihadapkan pada beberapa tantangan, seperti integritas jaringan yang terlalu terpusat, biaya dan kompleksitas tinggi, perubahan budaya, pemahaman yang diperlukan, serta dukungan pihak terkait. Keamanan data, terutama privasi pengguna, juga menjadi masalah karena sifat publik dari ledger blockchain. Diperlukan strategi cermat untuk meningkatkan privasi tanpa mengurangi keunggulan keamanan blockchain. Dalam kajian ini menggunakan metode kualitatif deskriptif dan pendekatan studi kasus. Dalam konteks implementasi teknologi blockchain dalam keamanan data di PUSTIPADA UINSU secara komprehensif. Kajian ini menggunakan teori kriptografi sebagai pendukung argumentasi penelitian. Teknik pengumpulan data kajian ini melalui wawancara, observasi langsung, dan analisis dokumen. Analisis data dilakukan dengan mempertimbangkan faktor teknis, sosial, dan infrastruktur. Dalam mempengaruhi keberhasilan implementasi. Hasilnya teknologi blockchain, yang berbasis pada kriptografi, menawarkan prospek signifikan untuk diadopsi dalam beragam sektor, termasuk pendidikan. Dalam konteks spesifik database kampus atau PUSTIPADA UINSU, penerapan teknologi blockchain dapat berkontribusi signifikan dalam peningkatan proteksi dan integritas data. Beberapa aspek penting yang perlu dipertimbangkan. a). Infrastruktur teknologi informasi yang ada harus mampu mendukung implementasi blockchain. b). Pertimbangan hukum dan regulasi yang berlaku juga harus diperhatikan. c). Pemahaman yang memadai tentang teknologi blockchain di antara pengguna dan pihak yang terlibat sangat penting.

Kata Kunci: Blockchain, Kriptografi, Keamanan Data, Pustipada UINSU.

1. PENDAHULUAN

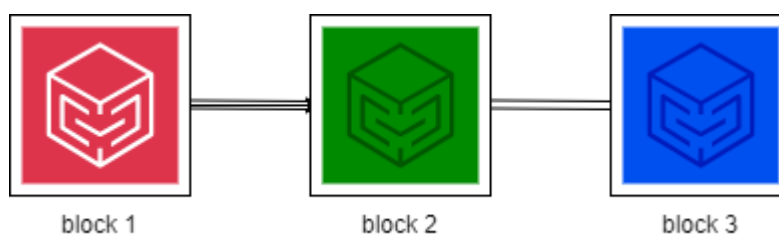
Proses perubahan signifikansi globalisasi menghantarkan digitalisasi yang membuka peluang besar, namun bersamaan dengan itu, risiko keamanan informasi pun meningkat. Metode keamanan tradisional tidak lagi mampu melawan serangan canggih. Terkhususnya, pada sektor teknologi. blockchain timbul sebagai solusi yang inovatif.

Blockchain menghasilkan opsional melalui sistem keamanan informasi yang kuat dan terjamin [1], [2]. Data disimpan dalam blok yang terhubung dan dienkripsi, menjamin integritas dan validitasnya. Sifat desentralisasi

blockchain membuatnya tahan terhadap manipulasi dan peretasan. Dalam era digitalisasi yang semakin pesat, keamanan data menjadi sangat penting untuk dijaga. Teknologi blockchain menawarkan solusi inovatif untuk meningkatkan keamanan data. Dengan prinsip dasar yang melibatkan penyimpanan data dalam blok terenkripsi yang saling terhubung dan terdistribusi di seluruh jaringan, teknologi ini mampu memberikan tingkat keamanan yang tinggi [3].

Implementasi teknologi blockchain menjadi fokus utama dalam berbagai sektor industri, termasuk keuangan, kesehatan, logistik, dan pendidikan. Di sektor pendidikan, teknologi ini dapat meningkatkan keamanan data mahasiswa, transkrip akademik, dan informasi penting lainnya. Meskipun demikian, tantangan seperti biaya tinggi, kompleksitas implementasi, serta perubahan budaya dan pemahaman yang diperlukan untuk adopsi teknologi ini, masih menjadi hambatan yang harus diatasi [4], [5].

Untuk mengatasi tantangan ini, diperlukan pendekatan yang holistik dan terpadu. Pihak yang terlibat dalam implementasi teknologi blockchain perlu memahami secara menyeluruh tentang teknologi ini, termasuk kelebihan, kekurangan, dan cara terbaik untuk mengimplementasikannya. Dalam konteks akademis, penelitian yang mendalam tentang implementasi teknologi blockchain dalam keamanan data dapat memberikan wawasan yang berharga bagi para akademisi, praktisi, dan pengambil keputusan dalam mengambil langkah-langkah yang tepat dalam mengamankan data mereka. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam pengembangan teknologi blockchain dan peningkatan keamanan data di berbagai sektor.



Gambar 1. Konsep Blockchain

Teknologi Blockchain mengandalkan enkripsi kode hash yang saling berkaitan antara satu blok dengan blok lainnya dalam jaringan yang terhubung. Hal ini menciptakan sebuah rantai blok yang telah diverifikasi. Dengan demikian, setiap data yang ada dalam blok memiliki kode unik yang dapat digunakan untuk memverifikasi keotentikan data tersebut. Ini adalah esensi dari teknologi Blockchain yang memastikan integritas dan keamanan data [6].

Hal ini, menjadi titik khusus yang dapat di adopsi oleh pihak sektor keuangan maupun pemerintahan untuk memperdayakan teknologi blockchain untuk meminimalisir adanya tracking pada transaksional keuangan ataupun dapat menjaga data-data khusus agar terhindari dari cracker. Pada dasarnya, teknologi blockchain dapat menjadi tolok ukur dalam menjaga sistem keamanan data user [7].Blockchain merupakan sebuah wadah yang menjadi tempat manifestasi penyimpanan data yang berbasis kriptografi yang memungkinkan serta menjaga data secara terenkripsi. Maka dari itu, blockchain acap kali sebagai protokol daripada proses transaksi yang mengedepankan esensial transparatif dan menghindari manipulatif data karena teknologi yang diimplementasikan pada blockchain sifatnya relatif aman.

Di sektor pendidikan, implementasi blockchain dapat meningkatkan keamanan data di kampus dan mengurangi ketergantungan pada otoritas pusat. Dengan mengimplementasikan sistem blockchain di pusat data atau pangkalan database kampus, kecil kemungkinannya data diri dari civitas kampus bocor dan tersebar secara luas. Dalam beberapa tahun terakhir, teknologi blockchain mulai diterapkan pada sistem keamanan informasi untuk meningkatkan integritas, privasi, dan keandalan data [8].

Kriptografi menjadi elemen penting dalam teknologi Blockchain, yang digunakan untuk mengamankan transaksi data, menjamin integritas, dan mencegah penyangkalan manipulasi. Prinsip kunci publik dan kunci privat dalam kriptografi sangat relevan untuk keamanan data dalam Blockchain. Dengan pemahaman mendalam tentang teori kriptografi, penelitian ini berpotensi untuk mengoptimalkan keamanan data

Blockchain pada dasarnya bertumpu pada sistem kriptografi yang menjadikan pusat sistem keamanan pada teknologi blockchain. Kriptografi adalah bidang ilmiah yang mempelajari teknologi enkripsi data. Kriptografi dibagi menjadi dua jenis, klasik dan modern, dengan kunci simetris dan asimetris [9]. Pada dasarnya, Kriptografi mengubah kode menjadi bentuk yang tidak dapat dipahami.

Terdapat dua proses dalam ilmu kriptografi, yaitu melakukan proses enkripsi dan dekripsi. Proses enkripsi memberi sandi plain text (pesan yang telah dienkripsi atau di berikan kode) ke cipher text (teks sandi). Pesan yaitu data atau informasi yang dapat dibaca dan dipahami dari maknanya [10]. Dengan peningkatan volume data yang ditransfer melalui jaringan, keamanan data menjadi sangat vital. Data yang tidak terlindungi dengan baik dapat diakses, dimodifikasi, atau dihapus oleh pihak yang tidak berwenang, atau bahkan digunakan untuk aktivitas kriminal. Teknologi enkripsi data muncul sebagai salah satu metode efektif untuk memastikan keamanan dan privasi data yang ditransfer melalui jaringan computer [11].

PUSTIPADA (Pusat Teknologi Informasi dan Pangkalan Data) UINSU adalah pusat data yang berisi informasi tentang civitas akademik Universitas Negeri Islam Sumatera Utara. Penelitian ini mengkaji penerapan teknologi blockchain dalam konteks keamanan data, terutama dalam lingkup PUSTIPADA UINSU. Dalam era digitalisasi yang berkembang pesat, keamanan data menjadi semakin penting. Metode keamanan tradisional tidak lagi cukup efektif melawan serangan canggih, terutama dalam sektor teknologi. Oleh karena itu, teknologi blockchain muncul sebagai solusi inovatif yang menjanjikan dalam meningkatkan keamanan data. Blockchain, dengan sifat terdesentralisasi dan enkripsi yang kuat, dapat memberikan tingkat keamanan yang tinggi terhadap manipulasi dan peretasan data. Studi kasus ini penting karena memberikan contoh aplikatif tentang bagaimana teknologi blockchain dapat diterapkan dalam sistem pendidikan untuk meningkatkan keamanan data. Implementasi teknologi ini memerlukan pemahaman yang mendalam dan kajian lebih lanjut untuk mengkaji lebih mendalam tentang implementasi teknologi Blockchain di PUSTIPADA UINSU.

2. Tinjauan Literatur

Fenomena emplicit yang sedang bergejolak dikala proses digitalisasi pada era teknologi ini acap kali menimbulkan polemik. Dalam konteks pendidikan, teknologi blockchain diharapkan dapat menjadi inovasi revolusioner dengan menawarkan sistem kriptografi dan desentralisasi. Isu privasi data, yang melibatkan perlindungan informasi pribadi dari penyalahgunaan dan akses tidak sah, menjadi fokus utama. Sebagai respons terhadap tantangan ini, adopsi teknologi blockchain telah muncul sebagai solusi potensial yang menjanjikan peningkatan signifikan dalam keamanan dan privasi data [12], [13].

Data rentan terdampak ancaman keamanan seperti Identity Theft, Phising, dan Dos Attack oleh pihak tidak berwenang. Laporan IBM Security mencatat biaya mean pada pelanggaran big data pada 2020 sebesar \$3.86 juta perinsiden. Hal ini memproyeksikan terkait urgensi dalam proteksi data dari ancaman tersebut [14]. Teknologi blockchain menjadi primadona sebagai solusi inovatif dalam sekuritas keamanan data. Studi ini fokus pada implementasi teknologi blockchain untuk meningkatkan keamanan data di PUSTIPADA UINSU.

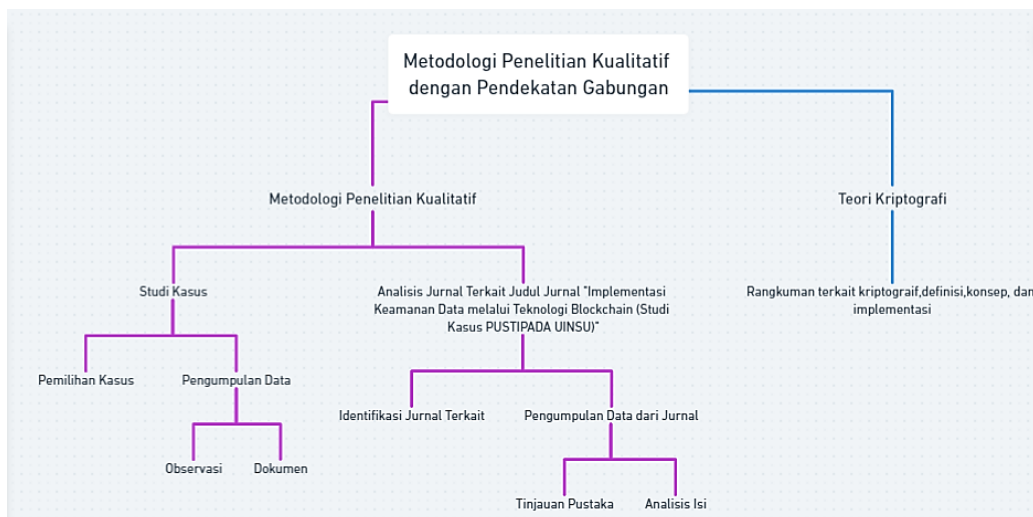
Blockchain berasaskan pada prinsip desentralisasi, yang mengimprovisasi kebutuhan akan entitas pusat dan memberikan dominan lebih kepada pengguna. Ini memiliki relevansi pada konteks keamanan dan privasi data, mengingat entitas pusat bisa menjadi titik lemah yang rentan terhadap serangan. Dalam blockchain, data disimpan secara tersebar di berbagai titik dalam jaringan, meningkatkan ketahanan terhadap serangan dan membuat manipulasi data menjadi sulit [15].

Dalam era digitalisasi, proteksi data menjadi imperatif mengingat risiko akses ilegal dan eksploitasi data. Di Indonesia, teknologi Blockchain telah muncul sebagai solusi inovatif untuk meningkatkan proteksi data. Entitas pemerintah dan swasta telah mempercepat adopsi teknologi ini dalam operasi sehari-hari mereka, termasuk proyek-proyek seperti validasi sertifikat pendidikan, penyimpanan data medis, dan sistem pembayaran. Meski demikian, implementasi Blockchain masih menghadapi hambatan, termasuk regulasi yang belum jelas, infrastruktur yang terbatas, dan kurangnya pemahaman tentang teknologi ini. Oleh karena itu, penting untuk terus berupaya mengatasi hambatan ini untuk memaksimalkan potensi teknologi Blockchain dalam menjaga proteksi data [16].

Dalam keamanan data melalui teknologi blockchain, menurut [17] membuat sebuah sistem keamanan berbasis teknologi blockchain dan kriptografi yang terintegrasi. Blockchain based Security Manager (BCSM) bertugas memastikan keaslian peristiwa dalam sistem, termasuk penyimpanan data besar, metadata, dan akses ke aset. BCSM juga mengelola blockchain dan berkomunikasi dengan entitas lain melalui saluran SSL/TLS yang aman. Untuk mengakses data, pengguna harus terotentikasi dan diotorisasi melalui berkas PL (Permission List) yang terkait dengan data yang diminta dari blockchain. Setelah mendapatkan otorisasi, manajer memperoleh data yang diminta menggunakan metadata dari blockchain [18]. Teknologi blockchain merupakan solusi efektif yang meningkatkan keamanan komunikasi, mencegah serangan spoofing, dan mempertahankan integritas data antar pihak yang berkomunikasi [19].

3. METODOLOGI

Dalam kajian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi kasus digunakan untuk mengkaji secara komprehensif tentang blockchain dan sistem keamanan data. Penelitian sebelumnya yang relevan dengan topik ini telah banyak membahas tentang sistem blockchain, kriptografi, dan keamanan data. Penggunaan teori kriptografi sebagai pendukung argumentatif kajian memberikan landasan teoritis yang kuat untuk analisis. Studi kasus yang digunakan dalam penelitian ini diharapkan dapat memberikan pemahaman mendalam tentang bagaimana blockchain dapat diterapkan dalam meningkatkan keamanan data dan menganalisis tantangan serta manfaatnya. Sehingga, penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam pemahaman dan penerapan teknologi blockchain dalam konteks keamanan data.



Gambar 2. Roadmap Penelitian

Pendekatan metodologi yang digunakan adalah studi kasus menurut [20], studi kasus memungkinkan peneliti untuk mendapatkan pemahaman yang mendalam tentang implementasi teknologi blockchain dalam keamanan data di PUSTIPADA UINSU. Data akan dikumpulkan melalui wawancara dengan pihak terkait di PUSTIPADA UINSU, observasi langsung terhadap proses implementasi teknologi blockchain, dan analisis dokumen terkait [21]. Analisis data akan dilakukan secara kualitatif dengan memperhatikan faktor-faktor yang mempengaruhi keberhasilan implementasi, seperti faktor teknis, sosial, dan infrastruktur. Hasil analisis akan digunakan untuk mengidentifikasi kelemahan yang ada dalam implementasi teknologi blockchain di PUSTIPADA UINSU dan memberikan rekomendasi perbaikan yang tepat.

4. HASIL DAN PEMBAHASAN

Pola Implementasi Blockchain Sistem Keamanan Data PUSTIPADA UINSU

Teknologi blockchain yang berlandaskan pada kriptografi menawarkan prospek signifikan untuk diadopsi dalam beragam sektor, termasuk pendidikan. Dalam konteks spesifik database kampus atau PUSTIPADA UINSU, penerapan teknologi blockchain dapat berkontribusi signifikan dalam peningkatan proteksi dan integritas data.

Namun, ada beberapa aspek penting yang perlu dipertimbangkan sebelum melakukan implementasi teknologi ini. Pertama, penting untuk memastikan bahwa infrastruktur teknologi informasi yang ada mampu mendukung implementasi blockchain. Kedua, pertimbangan hukum dan regulasi yang berlaku juga harus diperhatikan. Ketiga, pemahaman yang memadai tentang teknologi blockchain di antara pengguna dan pihak yang terlibat sangat penting.

Oleh karena itu, meskipun teknologi blockchain berbasis kriptografi menunjukkan potensi yang besar, implementasinya harus dipertimbangkan secara hati-hati dan melibatkan berbagai pihak yang relevan. Ini menunjukkan bahwa adopsi teknologi baru seperti ini bukanlah proses yang sederhana, tetapi memerlukan pemikiran dan perencanaan yang matang.

Akan tetapi, penting juga untuk mempertimbangkan biaya dan efisiensi implementasi teknologi blockchain. Meskipun teknologi ini menjanjikan keamanan dan integritas data yang tinggi, biaya untuk mengadopsi dan mengelola blockchain bisa menjadi faktor pembatas, terutama bagi institusi dengan anggaran terbatas seperti PUSTIPADA UINSU. Oleh karena itu, evaluasi menyeluruh terhadap manfaat dan biaya yang terkait dengan implementasi blockchain perlu dilakukan sebelum mengambil keputusan final. Dengan demikian, pemahaman yang holistik dan perencanaan yang cermat akan menjadi kunci sukses dalam menerapkan teknologi blockchain di lingkungan kampus atau institusi pendidikan, aspek-aspek vital dan krusial yang perlu dipertimbangkan dalam implementasi teknologi blockchain:

a). **Infrastruktur Teknologi Informasi**

Infrastruktur teknologi informasi (TI) diharuskan mendorong implementasi sistem blockchain [22]. Hal ini mencakup hardware (seperti server dan komputer), software (seperti sistem operasi dan aplikasi blockchain), dan network (seperti konektivitas internet dan protokol jaringan) yang menjadi tolak ukur untuk diintegrasikan. Infrastruktur TI yang kokoh dan sistematis sangat penting untuk memastikan bahwa sistem blockchain dapat beroperasi dengan efisien dan efektif.

b). **Pemahaman tentang Blockchain**

Ekosistem Blockchain yang kuat ini dikarenakan setiap teknologi yang beroperasi dalam network yang terdesentralisasi, acap kali membuatnya sulit untuk menemukan ruang bagi kegagalan pada titik tertentu [23]. User yang terlibat harus memiliki pemahaman yang komprehensif tentang teknologi blockchain. Ini mencakup bagaimana teknologi ini beroperasi, bagaimana menggunakannya, dan apa risikonya.

c). **Keamanan**

Salah satu fitur inti dari blockchain adalah "immutability", yang menjamin bahwa data tidak dapat diubah oleh individu. Setiap perubahan data memerlukan persetujuan dari konsensus jaringan, memastikan keamanan dan integritas data [24]. Akan tetapi, Blockchain mempunyai daya lebih maupun kurang terkhususnya dari aspek keamanan. Arsitektur ini memiliki kelemahan, yaitu risiko terancamnya kerahasiaan data jika terindikasi aktivitas peretasan [25]. Meskipun blockchain menawarkan tingkat keamanan yang tinggi melalui fitur "immutability" yang memastikan integritas data, namun teknologi ini juga memiliki kelemahan yang perlu diperhatikan. Salah satunya adalah risiko terancamnya kerahasiaan data jika terjadi aktivitas peretasan. Hal ini menunjukkan bahwa meskipun blockchain memberikan keamanan terhadap perubahan data yang tidak sah, namun kerahasiaan data masih memerlukan perhatian khusus dalam implementasinya. Oleh karena itu, pengelolaan keamanan data yang komprehensif dan terintegrasi tetap menjadi kunci dalam mengimplementasikan teknologi blockchain di berbagai sektor, termasuk di lembaga pendidikan tinggi seperti PUSTIPADA UINSU.

Tabel 1. Kekurangan Blockchain Pada Proteksi Data

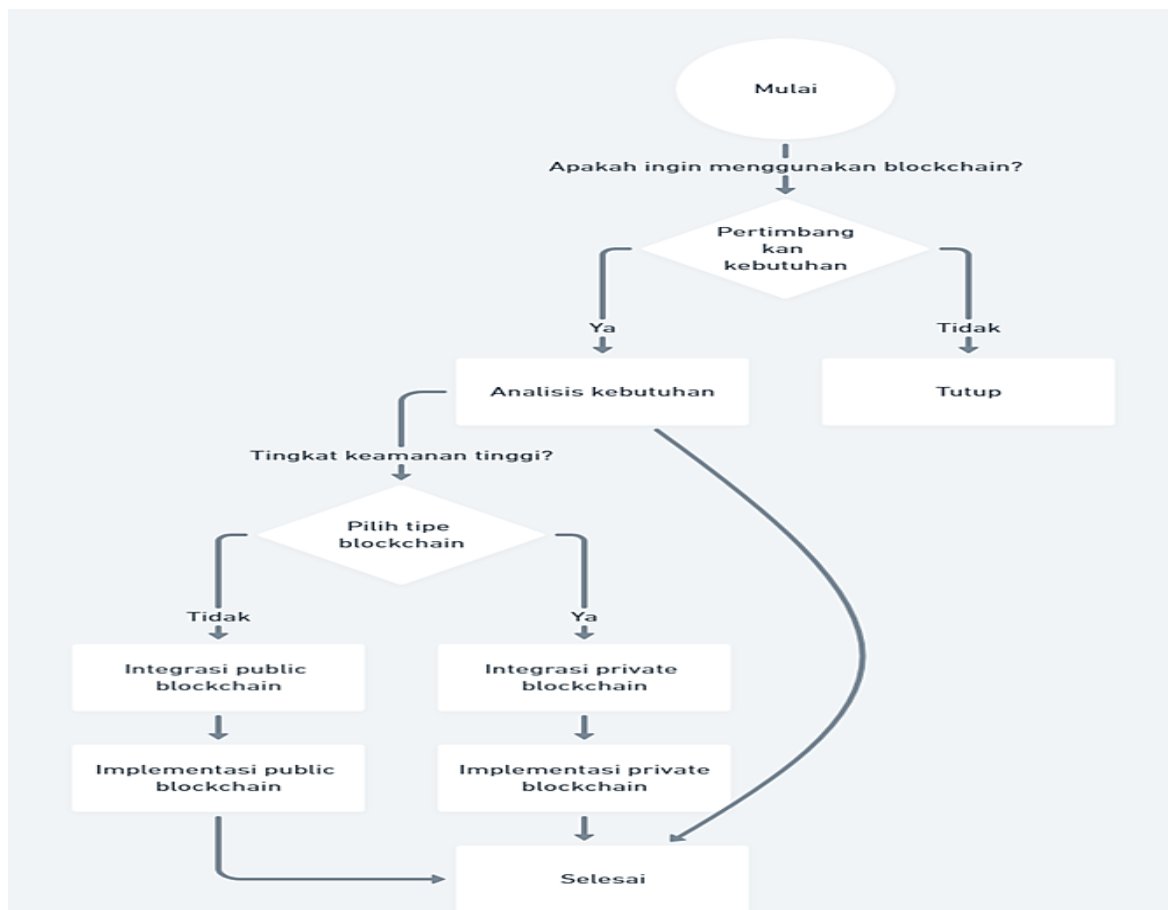
No	Kekurangan	Deskripsi
1	Sulit Modifikasi Data	Modifikasi data pada blockchain menantang dan kompleks. Kesalahan atau perubahan memerlukan persetujuan mayoritas partisipan, yang bisa memperlambat proses adaptasi.
2	Ketergantungan pada Kunci	Ketergantungan pada kunci pribadi menimbulkan risiko tinggi kehilangan akses aset. Kehilangan kunci atau lupa dapat mengakibatkan hilangnya aset atau data yang permanen.
3	Karakteristik Publik	Sifat publik dari ledger blockchain mengancam privasi pengguna. Informasi transaksi dapat diidentifikasi dan dianalisis oleh pihak yang tidak berwenang.
4	Integrasi Data	Integrasi dengan sistem lain sulit karena kurangnya standar konsisten. Perbedaan implementasi antara blockchain memerlukan upaya tambahan dalam integrasi.

Berdasarkan uraian pada tabulasi diatas dapat disaksikan bersama meskipun memiliki kelebihan blockchain pada dasarnya sebuah teknologi yang memiliki celah kelemahan pada system keamanannya. Oleh karena itu, berikut rangkuman kekurangan pada blockchain:

1. dalam keamanan dan integritas data, juga menghadapi beberapa kekurangan yang signifikan. a). Karakteristik immutability dalam teknologi blockchain sangat dihargai karena meningkatkan keamanan dan integritas data dengan membuatnya permanen dan tidak dapat diubah, namun membawa tantangan dalam adaptasi dan koreksi data. b). Immutability mempersulit perubahan data yang dibutuhkan karena kesalahan input atau perubahan kondisi, seperti dalam kontrak cerdas yang dapat menyebabkan kerugian finansial jika berisi kesalahan [26].
2. Proses konsensus untuk mengubah data di blockchain seringkali mahal dan memakan waktu, menghambat inovasi dan responsivitas terhadap perubahan. a). Ketergantungan pada persetujuan mayoritas juga menciptakan dinamika kekuasaan yang dapat mempengaruhi keputusan jaringan. Oleh karena itu, b). Sementara immutability membantu mencegah manipulasi, ia juga membatasi fleksibilitas sistem dan memerlukan penelitian lebih lanjut serta pengembangan solusi untuk koreksi terkontrol yang akan memungkinkan aplikasi blockchain yang lebih luas dan adaptif [27].
3. Ketergantungan teknologi blockchain pada kunci kriptografi adalah aspek fundamental yang memperkuat keamanan dan kerahasiaan data, namun menghadirkan risiko yang signifikan. a). Kehilangan atau pencurian kunci kriptografi bisa mengakibatkan kehilangan akses permanen ke aset digital, tanpa harapan pemulihan. b). Karena mekanisme yang ada berisiko mengompromikan keamanan [28].
4. Risiko ini diperparah oleh serangan cyber yang semakin canggih, seperti phishing dan malware, yang dapat mencuri kunci dan mengancam integritas transaksi. Selain itu, a). Pengelolaan kunci yang memadai sering kali terhambat oleh ketiadaan pengetahuan atau sumber daya yang cukup, menciptakan disparitas keamanan di antara pengguna [29]. Oleh karena itu, pentingnya penelitian. b). Untuk mengembangkan mekanisme pemulihan kunci yang lebih aman atau alternatif autentikasi yang tidak mengorbankan keamanan demi aksesibilitas. Hal ini akan, c). Menentukan kemampuan blockchain untuk menjadi lebih inklusif dan tahan terhadap ancaman.

5. Ledger publik pada blockchain meningkatkan transparansi dan memperkuat kepercayaan dan akuntabilitas, tetapi juga memunculkan dilema privasi signifikan [30]. Sifat terbukanya memungkinkan siapa saja untuk mengakses dan menganalisis transaksi, yang dapat mengancam kerahasiaan pengguna dan memfasilitasi penggunaan data untuk tujuan tidak etis. Meskipun transaksi dienkripsi, detail seperti jumlah dan waktu tetap terlihat, meningkatkan risiko eksposur data pribadi. Selanjutnya, a). Ketidakmungkinan menghapus atau mengubah data dalam blockchain bertentangan dengan regulasi seperti GDPR yang mendukung hak untuk dilupakan. Oleh karena itu, meskipun transparansi blockchain memberikan banyak manfaat, juga penting untuk b). Mengembangkan solusi yang memperkuat privasi tanpa mengorbankan keunggulan ini, guna mencapai keseimbangan antara kebutuhan transparansi dan perlindungan privasi.
6. Integrasi data antara blockchain dan sistem lain menghadapi tantangan kompleks akibat perbedaan prinsip desentralisasi, kurangnya standar konsisten, dan kebutuhan untuk menyelaraskan keamanan serta privasi [31]. a). Keamanan tinggi yang ditawarkan oleh blockchain memerlukan strategi yang cermat untuk memastikan konsistensi dengan regulasi privasi seperti GDPR, sementara juga memerlukan investasi dalam sumber daya teknis dan operasional. Penelitian dan pengembangan lebih lanjut diperlukan untuk b). Mengatasi hambatan ini dan memfasilitasi integrasi yang efisien antara blockchain dan infrastruktur IT yang sudah ada.

7.



Gambar 3. Proses Pengambilan Keputusan Dalam Implementasi Teknologi Blockchain

Berdasarkan keterangan alur dari diagram alir diatas yang memaparkan proses pengambilan keputusan penting dalam implementasi blockchain. Dimulai dengan pertanyaan fundamental tentang keinginan untuk menggunakan blockchain, diagram ini menekankan bahwa keputusan tersebut harus didasarkan pada kebutuhan spesifik, bukan sekadar tren teknologi . Jika keputusan diambil untuk melanjutkan dengan blockchain, analisis

kebutuhan dan tingkat keamanan menjadi langkah kritis berikutnya. Dalam konteks PUSTIPADA, ini melibatkan evaluasi data yang perlu diamankan, tingkat risiko, dan persyaratan keamanan lainnya. Selanjutnya, berdasarkan kebutuhan keamanan, pilihan antara blockchain publik dan pribadi harus dibuat. Ini menunjukkan bahwa jenis blockchain yang dipilih harus sesuai dengan kebutuhan keamanan. Dalam konteks PUSTIPADA, ini bisa berarti mempertimbangkan trade-off antara transparansi (blockchain publik) dan kontrol (blockchain pribadi). Secara keseluruhan, diagram alir ini memberikan kerangka kerja yang komprehensif untuk memahami dan menganalisis implementasi blockchain dalam konteks keamanan data.

Implementasi teknologi blockchain dalam meningkatkan keamanan data, seperti yang terjadi pada PUSTIPADA UINSU, adalah langkah inovatif namun kompleks. Dalam teori kriptografi, penggunaan blockchain dijelaskan sebagai sistem terdistribusi yang menggunakan kriptografi untuk mengamankan transaksi dan data. Namun, keberhasilan implementasi blockchain tergantung pada sejumlah faktor kritis sebagai berikut:

- a) Keberhasilan blockchain dalam keamanan data tergantung pada integritas jaringan. Jika jaringan terlalu terpusat, risiko keamanan meningkat karena potensi manipulasi data oleh pihak yang memiliki kendali.
- b) Biaya dan kompleksitas implementasi blockchain dapat menjadi hambatan. Mengelola blockchain memerlukan sumber daya yang signifikan, termasuk biaya operasional dan keamanan. Selain itu, perubahan budaya dan pemahaman yang diperlukan untuk adopsi teknologi ini juga memerlukan investasi waktu dan sumber daya yang besar.
- c) Keberhasilan implementasi blockchain juga tergantung pada dukungan dari pihak terkait, termasuk manajemen dan staf. Kegagalan untuk mendapatkan dukungan ini dapat menghambat implementasi yang efektif. Dalam konteks PUSTIPADA UINSU, analisis kritis terhadap implementasi blockchain perlu memperhitungkan faktor-faktor ini untuk mengidentifikasi keberhasilan, kegagalan, dan rekomendasi perbaikan yang tepat.

Penerapan teknologi blockchain dalam meningkatkan keamanan data, seperti yang terjadi pada PUSTIPADA UINSU, adalah langkah inovatif namun kompleks. Dalam teori kriptografi, penggunaan blockchain dijelaskan sebagai sistem terdistribusi yang menggunakan kriptografi untuk mengamankan transaksi dan data. Namun, keberhasilan implementasi blockchain tergantung pada sejumlah faktor kritis. Terutama, keberhasilan blockchain dalam keamanan data tergantung pada integritas jaringan. Jika jaringan terlalu terpusat, risiko keamanan meningkat karena potensi manipulasi data oleh pihak yang memiliki kendali. Faktor kedua adalah biaya dan kompleksitas implementasi blockchain yang dapat menjadi hambatan. Mengelola blockchain memerlukan sumber daya yang signifikan, termasuk biaya operasional dan keamanan. Perubahan budaya dan pemahaman yang diperlukan untuk adopsi teknologi ini juga memerlukan investasi waktu dan sumber daya yang besar. Faktor ketiga adalah dukungan dari pihak terkait, termasuk manajemen dan staf. Kegagalan untuk mendapatkan dukungan ini dapat menghambat implementasi yang efektif. Dalam konteks PUSTIPADA UINSU, analisis kritis terhadap implementasi blockchain perlu memperhitungkan faktor-faktor ini untuk mengidentifikasi keberhasilan, kegagalan, dan rekomendasi perbaikan yang tepat.

Akan tetapi, patut diperhitungkan dalam implementasi teknologi blockchain dalam konteks PUSTIPADA UINSU juga perlu memperhatikan aspek keamanan data yang melibatkan privasi pengguna. Meskipun blockchain menawarkan keamanan tinggi melalui fitur "immutability", yang memastikan integritas data, namun kerahasiaan data juga harus dijaga dengan ketat. Sifat publik dari ledger blockchain dapat mengancam privasi pengguna karena informasi transaksi dapat diakses dan dianalisis oleh pihak yang tidak berwenang. Oleh karena itu, strategi yang cermat diperlukan untuk memperkuat privasi tanpa mengorbankan keunggulan keamanan yang ditawarkan oleh blockchain. Solusi ini harus mencapai keseimbangan antara kebutuhan transparansi dan perlindungan privasi yang diperlukan oleh regulasi seperti GDPR.

Selain itu, integrasi data antara blockchain dan sistem lain di PUSTIPADA UINSU juga menghadapi tantangan kompleks. Perbedaan prinsip desentralisasi antara blockchain dan infrastruktur TI yang sudah ada, kurangnya standar konsisten, dan kebutuhan untuk menyelaraskan keamanan serta privasi adalah faktor-faktor yang perlu dipertimbangkan dengan matang. Pengelolaan yang tepat dalam mengintegrasikan blockchain dengan

infrastruktur TI yang ada adalah kunci untuk memastikan bahwa keamanan data terjaga dengan baik. Diperlukan upaya tambahan dalam penelitian dan pengembangan untuk mengatasi hambatan ini dan memfasilitasi integrasi yang efisien antara blockchain dan infrastruktur TI yang sudah ada di PUSTIPADA UINSU.

5. KESIMPULAN

Berdasarkan hasil penelitian di atas dapat dijelaskan bahwa globalisasi dan digitalisasi telah membawa peluang besar namun juga meningkatkan risiko keamanan informasi, terutama dalam sektor teknologi. Metode keamanan tradisional tidak lagi cukup efektif melawan serangan canggih. Untuk mengatasi tantangan ini, teknologi blockchain muncul sebagai solusi inovatif dengan sistem keamanan informasi yang kuat dan terjamin. Blockchain menyimpan data dalam blok terhubung dan dienkripsi, memastikan integritas dan validitasnya. Desentralisasi blockchain membuatnya tahan terhadap manipulasi dan peretasan. Implementasi blockchain memiliki potensi besar dalam berbagai sektor industri, termasuk keuangan, kesehatan, logistik, dan pendidikan. Di sektor pendidikan, blockchain dapat meningkatkan keamanan data mahasiswa, transkrip akademik, dan informasi penting lainnya. Namun, implementasi blockchain masih dihadapkan pada beberapa tantangan, termasuk biaya tinggi, kompleksitas implementasi, serta perubahan budaya dan pemahaman yang diperlukan untuk adopsi teknologi ini. Oleh karena itu, implementasi teknologi blockchain di PUSTIPADA UINSU dapat memberikan kontribusi signifikan dalam peningkatan proteksi dan integritas data, tetapi memerlukan pemahaman yang mendalam, infrastruktur TI yang memadai, serta pemikiran dan perencanaan yang matang. Meskipun memiliki kelebihan, blockchain juga memiliki beberapa kelemahan, seperti kesulitan modifikasi data, ketergantungan pada kunci, karakteristik publik yang mengancam privasi, dan kesulitan integrasi dengan sistem lain.

6. DAFTAR PUSTAKA

- [1] A. Arwani and U. Priyadi, "Eksplorasi Peran Teknologi Blockchain dalam Meningkatkan Transparansi dan Akuntabilitas dalam Keuangan Islam: Tinjauan Sistematis," *J. Ekon. BISNIS DAN Manaj.*, vol. 2, no. 2, pp. 23–37, Mar. 2024, doi: 10.59024/jise.v2i2.653.
- [2] P. W. Susanto and W. M. Ashari, "Penerapan Teknologi Blockchain pada Transaksi Online Shop," *Al Qalam J. Ilm. Keagamaan Dan Kemasyarakatan*, vol. 18, no. 1, p. 654, Jan. 2024, doi: 10.35931/aq.v18i1.2778.
- [3] A. Ramadhani, D. A. Ananda, and Z. Azmi, "Teknologi Blockchain dan Sistem Akuntansi: Potensi dan Tantangan," vol. 1, no. 1, 2024.
- [4] I. K. Najibulloh and L. Rahmalia, "PENERAPAN TEKNOLOGI BLOCKCHAIN DALAM INDUSTRI KEUANGAN SYARIAH: TANTANGAN DAN PELUANG," *J-EBI J. Ekon. Bisnis Islam*, vol. 3, no. 01, Mar. 2024, doi: 10.57210/j-ebi.v3i01.295.
- [5] A. Nanda Sari and T. Gelar, "BLOCKCHAIN: TEKNOLOGI DAN IMPLEMENTASINYA," *J. Mnemon.*, vol. 7, no. 1, pp. 63–70, Mar. 2024, doi: 10.36040/mnemonic.v7i1.6961.
- [6] P. A. Sunarya, "Penerapan Sertifikat pada Sistem Keamanan menggunakan Teknologi Blockchain," 2022.
- [7] Djumadi, "Teknologi Blockchain dalam Perspektif Ekonomi Islam / Keuangan Islam," *Al-Kharaj J. Ekon. Keuang. Bisnis Syariah*, vol. 6, no. 4, pp. 4335–4351, Feb. 2024, doi: 10.47467/alkharaj.v6i4.887.
- [8] I. E. Maulani, T. Herdianto, D. F. Syawaludin, and M. O. Laksana, "PENERAPAN TEKNOLOGI BLOCKCHAIN PADA SISTEM KEAMANAN INFORMASI," vol. 3, no. 2, 2023.
- [9] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains Dan Komput.*, vol. 2, no. 01, pp. 163–171, Mar. 2022, doi: 10.47709/jpsk.v2i01.1390.
- [10] R. Oktafiani, E. I. H. Ujianto, and R. Rianto, "Kombinasi Algoritma Kriptografi Vigenere Cipher dan SHA256 untuk Keamanan Basis Data," *J. Sist. Komput. Dan Inform. JSON*, vol. 4, no. 3, p. 433, Mar. 2023, doi: 10.30865/json.v4i3.5583.
- [11] N. W. Hidayatulloh, M. Tahir, H. Amalia, N. A. Basyar, A. F. Prianggara, and M. Yasin, "Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data," vol. 3, no. 1, 2023.
- [12] Samlan Hi. Ahmad, Muhammad Yaumi, Chadijah, and Majida Faruk, "BLOCKHAIN DALAM PEMBELAJARAN ABAD 21," *Aksara Kawanua J. Ilm. Multidisiplin*, vol. 2, no. 2, pp. 65–73, 2023.
- [13] Z. Munawar, N. Indah Putri, I. Iswanto, and D. Widhiantoro, "ANALISIS KEAMANAN PADA TEKNOLOGI BLOCKCHAIN," *Infotronik J. Teknol. Inf. Dan Elektron.*, vol. 8, no. 2, p. 67, Dec. 2023, doi: 10.32897/infotronik.2023.8.2.2062.

- [14] M. A. D. Yuda and S. Watini, "Implementation of Blockchain Technology as the Latest Solution to Improve Data Security and Integrity," *Int. Trans. Educ. Technol. ITEE*, vol. 2, no. 1, 2023.
- [15] I. E. Maulani, T. Herdianto, D. F. Syawaludin, and M. O. Laksana, "PENERAPAN TEKNOLOGI BLOCKCHAIN PADA SISTEM KEAMANAN INFORMASI," *J. Sos. Dan Teknol. SOSTECH*, vol. 3, no. 2, 2023.
- [16] T. W. E. Suryawijaya, "Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia," *J. Studi Kebijak. Publik*, vol. 2, no. 1, pp. 55–68, May 2023, doi: 10.21787/jskp.2.2023.55-68.
- [17] H. E. Alhazmi, F. E. Eassa, and S. M. Sandokji, "Towards Big Data Security Framework by Leveraging Fragmentation and Blockchain Technology," *IEEE Access*, vol. 10, pp. 10768–10782, 2022, doi: 10.1109/ACCESS.2022.3144632.
- [18] C. Satya Wardhana, "Implementasi Teknologi Blockchain Dalam Optimalisasi Keamanan Database Penduduk Di Kementerian Dalam Negeri," *Action Res. Lit.*, vol. 8, no. 4, pp. 642–648, Apr. 2024, doi: 10.46799/ar.v8i4.305.
- [19] D. Firmansyah, "PENERAPAN TEKNOLOGI BLOCKCHAIN UNTUK MENGATASI SERANGAN MAN IN THE MIDDLE," vol. 1, no. 1, 2023.
- [20] J. W. Creswell, *Research Design: Pendekatan Kualitatif, Kuantitatif, dan Mixed*. Pustaka Pelajar, 2010.
- [21] Matthew B. Miles, A. Michael Huberman, and Johnny Saldaña, *Qualitative Data Analysis A Methods Sourcebook Edition 4, 4th ed.* Arizona State University, USA: SAGE Publications, Inc, 2019.
- [22] Iswanto, N. I. Putri, Z. Munawar, R. Komalasari, and Dandun Widhiantoro, "Pemanfaatan Teknologi Blockchain di Bidang Pendidikan," *TEMATIK*, vol. 9, no. 2, pp. 171–181, Dec. 2022, doi: 10.38204/tematik.v9i2.1082.
- [23] U. Rahardja, Q. Aini, M. Yusup, and A. Edliyanti, "Penerapan Teknologi Blockchain Sebagai Media Pengamanan Proses Transaksi E-Commerce," *CESS J. Comput. Eng. Syst. Sci.*, vol. 5, no. 1, p. 28, Jan. 2020, doi: 10.24114/cess.v5i1.14893.
- [24] F. D. Wihartiko, S. Nurdianti, A. Buono, and E. Santosa, "Blockchain dan Kecerdasan Buatan dalam Pertanian : Studi Literatur," *J. Teknol. Inf. Dan Ilmu Komput.*, vol. 8, no. 1, p. 177, Feb. 2021, doi: 10.25126/jtiik.0814059.
- [25] J. O. Y. Tampubolon, A. Bhawiyuga, and R. A. Siregar, "Implementasi Blockchain berbasis BigchainDB untuk Menjamin Keamanan Data dalam Sistem Pencatatan Rekam Medis," vol. 6, no. 3, 2022.
- [26] A. M. Alqahtani and A. Algarni, "A Survey on Blockchain Technology Concepts, Applications and Security," *Int. J. Adv. Comput. Sci. Appl.*, 2023, [Online]. Available: <https://api.semanticscholar.org/CorpusID:257394924>
- [27] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain Res. Appl.*, vol. 3, no. 2, p. 100067, 2022, doi: <https://doi.org/10.1016/j.bcra.2022.100067>.
- [28] I. I. Nugroho, R. Pratiwi, and S. R. A. Zahro, "Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia," *Ikut. Penulis Mhs. Huk. Indones. Law J.*, 2021, [Online]. Available: <https://api.semanticscholar.org/CorpusID:247092899>
- [29] S. Rashidibajgan and T. Hupperich, "Utilizing blockchains in opportunistic networks for integrity and confidentiality," *Blockchain Res. Appl.*, vol. 5, no. 1, p. 100167, 2024, doi: <https://doi.org/10.1016/j.bcra.2023.100167>.
- [30] I. P. Dewi, P. Herwanto, H. Wicaksono, and Rosida, "Analisis Faktor-faktor yang Mempengaruhi Penerimaan Teknologi Blockchain dalam Industri Akuntansi," *Inf. J. Inform. Dan Sist. Inf.*, 2023, [Online]. Available: <https://api.semanticscholar.org/CorpusID:258922923>
- [31] S. Bansod and L. L. Ragha, "Blockchain Technology: Applications and Research Challenges," 2020 *Int. Conf. Emerg. Technol. INCET*, pp. 1–6, 2020.