

Meningkatkan Privasi dan Kepercayaan dalam Platform Media Sosial: Penerapan Teknologi Blockchain dan Pendekatan Kualitatif

Raihan Syafawi Batubara^{1*}, Rizki Julyanda², Supiyandi³

^{1,2,3}Fakultas Sains dan Teknologi, Program Studi Teknologi Informasi, Universitas Pembangunan Panca Budi, Medan, Indonesia

Email: ^{1*}raihausyafawi44@gmail.com, ²rizkijulyanda@gmail.com, ³supiyandi@dosen.pancabudi.ac.id

(* Email Corresponding Author: raihausyafawi44@gmail.com)

Dikirim: 27 April 2025 | Diterima: 3 Juli 2025 | Dipublish: 31 Juli 2025

Abstrak

Media sosial telah menjadi bagian yang terpenting di kehidupan modern kita saat ini, namun *platform* media sosial sering dihadapkan pada berbagai tantangan privasi dan kepercayaan pengguna. Teknologi *blockchain*, dengan karakteristik desentralisasi, keamanan, dan transparansi, menawarkan solusi potensial untuk mengatasi tantangan ini. Tujuan utama dari penelitian ini adalah berkontribusi untuk memahami dan mengatasi tantangan privasi dan kepercayaan dalam platform media sosial. Studi ini berfokus pada memanfaatkan teknologi *blockchain* untuk menciptakan lingkungan media sosial yang lebih aman dan lebih transparan. Diharapkan *blockchain* dapat membawa perubahan positif dalam membangun media sosial yang lebih aman dan transparan. Metodologi penelitian mengadopsi pendekatan kualitatif, khususnya metode deskriptif kualitatif. Metode ini melibatkan menghasilkan data deskriptif dalam bentuk tertulis atau lisan dari individu dan perilaku yang diamati. Hasil penelitian ini menunjukkan bahwa studi ini mengusulkan kerangka konseptual yang komprehensif untuk meningkatkan privasi dan kepercayaan pada *platform* media sosial melalui teknologi *blockchain*. Temuan menunjukkan bahwa *blockchain* dapat menawarkan solusi signifikan untuk pengumpulan data invasif, keamanan informasi, dan transparansi manajemen data. Dengan membangun kontrol data pengguna yang lengkap, identitas digital yang aman dan terverifikasi, serta tata kelola platform yang transparan dan akuntabel, implementasi *blockchain* diharapkan dapat memberikan pengguna kontrol penuh atas data mereka, membangun identitas digital yang aman, dan meningkatkan transparansi dalam pengambilan keputusan dan operasi *platform*.

Kata Kunci: Privasi, Teknologi Blockchain, Media Sosial, Tata Kelola Platform, Platform, Keamanan Data, Identitas Digital, Transparansi.

Abstract

Social media has become an important part of our modern lives today, but social media platforms are often faced with various challenges regarding user privacy and trust. Blockchain technology, with its characteristics of decentralization, security, and transparency, offers a potential solution to overcome these challenges. The main goal of this research is to contribute to understanding and overcoming the challenges of privacy and trust in social media platforms. This study focuses on leveraging blockchain technology to create a safer and more transparent social media environment. It is hoped that blockchain can bring positive changes in developing safer and more transparent social media. The research methodology adopts a qualitative approach, especially qualitative descriptive methods. This method involves generating descriptive data in written or verbal form from individuals and observed behavior. The results of this research indicate that this study proposes a comprehensive conceptual framework for enhancing privacy and trust on social media platforms through blockchain technology. The findings suggest that blockchain can offer significant solutions to invasive data collection, information security, and data management transparency. By establishing complete user data control, secure and verifiable digital identities, and transparent and accountable platform governance, blockchain implementation is expected to give users full control over their data, build secure digital identities, and increase transparency in decision-making and operations platforms.

Keywords: Privacy, Blockchain Technology, Social Media, Platform Governance, Data Security, Digital Identity, Transparency.

1. PENDAHULUAN

Perkembangan teknologi media sosial dan informasi memiliki impact yang besar terhadap kehidupan kita sehari-hari, hal ini menyebabkan ketergantungan pada penggunaan media sosial. Namun, perkembangan ini mengakibatkan kita harus menghadapi tantangan untuk melindungi privasi setiap individu[1]. Transformasi teknologi yang tengah berlangsung saat ini memaksa baik individu maupun organisasi untuk melakukan adaptasi digital, dan transformasi ini merupakan upaya teknologi digital untuk mengubah proses yang ada dan menciptakan cara baru[2]. Teknologi blockchain memiliki potensi yang besar untuk meningkatkan keamanan data. Data yang tersimpan pada Blockchain, ditransfer secara peer-to-peer dengan mendistribusikan database ke beberapa lokasi, untuk mengurangi ketergantungan pada satu server tunggal. Implementasi sistem keamanan kolektif pada blockchain menjadikannya pilihan yang sangat efektif dalam menjaga integritas data[3]. Platform media sosial adalah media di mana orang berkumpul dan bebas mengekspresikan pendapat, sehingga platform ini dapat menawarkan wawasan yang berarti tentang perspektif publik terhadap perubahan sosial dan selama situasi krisis[4]. Blockchain berfungsi sebagai sistem penyimpanan data digital yang terhubung melalui kriptografi, menawarkan keunggulan sebagai basis data

terdistribusi yang tidak dapat dimanipulasi dan aman dalam hal validitas dan privasi[5]. Keamanan data menjadi fokus utama dalam pengembangan blockchain, dengan lapisan-lapisan keamanan seperti hash, private-public key, dan distribusi data P2P yang menjadikannya ideal untuk penyimpanan data yang dapat dipercaya dan minim risiko manipulasi[6].

Blockchain pertama kali dikenal melalui cryptocurrency seperti Bitcoin, teknologi ini menawarkan potensi besar dalam transformasi sektor digital. Bitcoin, diciptakan berdasarkan teknologi Block-chain oleh Satoshi Nakamoto sekitar tahun 2008, telah mempopulerkan dan mengubah pandangan terhadap teknologi blockchain secara luas[7]. Di era sekarang, Social Media telah menjadi bagian yang tak dapat terpisahkan dari kehidupan kita saat ini. Bagi banyak orang, media sosial telah menjadi sumber hiburan, edukasi, dan koneksi dengan orang lain di seluruh dunia. Namun, di balik gemerlapnya, media sosial tradisional sering kali dihadapkan pada berbagai tantangan yang mengkhawatirkan, terutama terkait privasi dan kepercayaan pengguna. Kekhawatiran ini meliputi pengumpulan Data yang Invasif yaitu platform media sosial tradisional mengumpulkan data pengguna dalam jumlah besar, termasuk informasi pribadi seperti profil, aktivitas online, dan interaksi dengan pengguna lain. Data ini sering kali dikumpulkan tanpa persetujuan eksplisit pengguna dan digunakan untuk berbagai tujuan, seperti periklanan bertarget, pengembangan produk, dan analisis perilaku pengguna. Selain itu juga terkait pelanggaran privasi yaitu kasus kebocoran data dan penyalahgunaan data pribadi pengguna sering kali terjadi di platform media sosial tradisional. Hal ini dapat menyebabkan pencurian identitas, penipuan, dan kerugian finansial bagi pengguna. Dan juga kekhawatiran terkait penyebaran Misinformasi: Platform media sosial tradisional menjadi wadah bagi penyebaran misinformasi dan berita palsu. Hal ini dapat berdampak negatif pada opini publik, memicu perselisihan sosial, dan bahkan mengganggu proses demokrasi[8].

Penggunaan teknologi informasi yang semakin luas dan rumit pada saat ini, memunculkan berbagai ancaman serta tantangan dalam menjaga keamanan data pribadi setiap individu pada social media. Hal ini menyadarkan kita bahwa saat ini kita membutuhkan solusi yang efektif dan efisien untuk keamanan data setiap orang agar terhindar dari serangan, kebocoran data serta pencurian data yang bisa merugikan banyak pihak. Tujuan jurnal ini ialah memperkenalkan teknologi blockchain kepada khalayak sebab teknologi ini mampu untuk meningkatkan keamanan data[9]. Kekhawatiran privasi dan kepercayaan ini mendorong para peneliti dan developer untuk mencari solusi baru dalam meningkatkan keamanan dan privasi pengguna di platform media sosial. Teknologi blockchain, yang mendasari cryptocurrency seperti Bitcoin, muncul sebagai solusi potensial yang menjanjikan. Teknologi blockchain, dengan karakteristik desentralisasi, keamanan, dan transparansi, menawarkan beberapa fitur yang dapat mengatasi tantangan privasi dan kepercayaan dalam media sosial:

a. Desentralisasi: Blockchain dikendalikan lebih dari satu entitas, fitur tersebut disalurkan ke jaringan komputer yang luas. Hal ini memberikan kontrol dan transparansi yang lebih besar kepada pengguna atas data mereka.

b. Keamanan: Blockchain menggunakan kriptografi yang kuat untuk mengamankan data dan transaksi, membuatnya tahan terhadap peretasan dan manipulasi.

c. Transparansi: Semua transaksi di blockchain telah tercatat dalam buku besar publik, yang mana buku tersebut siapa pun dapat mengaksesnya. Hal ini memungkinkan verifikasi dan audit yang mudah, meningkatkan akuntabilitas dan kepercayaan.

Jurnal ini mengusulkan kerangka konseptual yang komprehensif untuk meningkatkan privasi dan kepercayaan dalam platform media sosial melalui teknologi blockchain. Kerangka ini didasarkan pada tinjauan literatur yang ekstensif dan analisis mendalam tentang tantangan privasi dan kepercayaan dalam media sosial, serta potensi solusi yang ditawarkan oleh teknologi blockchain. Kerangka ini mencakup dua pilar utama diantaranya:

a. Kontrol Data Pengguna yang Lengkap: Pengguna harus memiliki kontrol penuh atas data mereka yang dikumpulkan oleh platform media sosial. Blockchain dapat memberikan setiap pengguna akses yang aman dan transparan ke data mereka, hak privasi yang kuat, dan portabilitas data. Hal ini membuat sistem lebih sulit dihack dan meminimalisir biaya transaksi karena tidak ada perantara yang diperlukan.

b. Identitas Digital yang Aman dan Terverifikasi: Pengguna harus memiliki identitas digital yang aman dan terverifikasi untuk berinteraksi dengan platform media sosial. Blockchain dapat digunakan untuk membangun identitas digital yang aman dan portabel, verifikasi identitas yang aman, dan pengendalian akses yang granular.

Keamanan teknologi blockchain sangat terjamin dengan penggunaan kriptografi yang kuat dan canggih. Setiap transaksi dalam blockchain dicatat secara permanen dan dilindungi, sehingga data sulit untuk dimanipulasi. Selain itu, blockchain mengharuskan setiap transaksi untuk disetujui oleh pengguna sebelum dimasukkan ke dalam rantai blok, meningkatkan keamanan secara signifikan[3]. Blockchain awalnya dikenal sebagai platform publik, namun sekarang ada berbagai jenis blockchain seperti consortium dan pribadi, yang dikembangkan oleh berbagai instansi untuk keperluan spesifik. Pemilihan jenis blockchain harus disesuaikan

dengan kebutuhan masing-masing kasus untuk implementasi yang tepat[10]. Blockchain memiliki 3 jenis yang berbeda, diantaranya adalah :

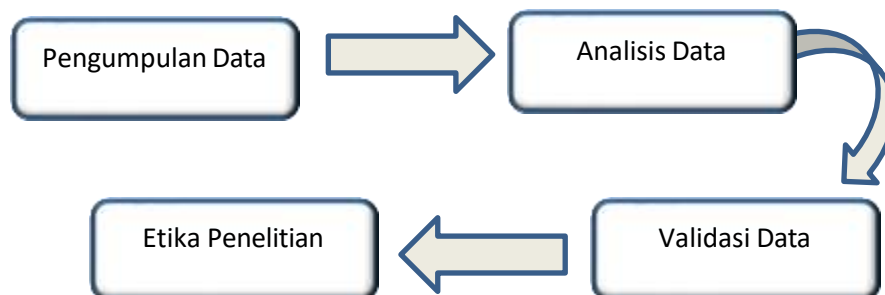
a. Public : Jenis blockchain merupakan jenis yang terbuka untuk umum dan dapat diakses oleh siapa pun. Contohnya adalah blockchain Bitcoin dan Ethereum. Setiap orang dapat mengirim transaksi, memverifikasi transaksi, dan bergabung sebagai node dalam jaringan ini. Informasi yang tersimpan pada blockchain public bersifat transparan dan dapat diakses oleh siapa pun.

b. Consortium : Jenis blockchain ini berada di antara blockchain public dan private. Dalam blockchain konsorsium, sekelompok organisasi atau entitas yang telah dipilih bekerja sama untuk mengendalikan jaringan blockchain, hingga transaksi pada blockchain bisa dibuat untuk umum atau hanya orang-orang tertentu yang memiliki akses.

c. Private : Jenis blockchain yang tidak bisa diakses oleh semua orang dan biasanya digunakan oleh lingkungan dalam perusahaan yang sangat menjaga data data nya. Jenis blockchain ini bersifat tertutup dan hanya ada satu pihak node saja yang bisa melakukan pembacaan dan pencatatan data[11].

Tujuan penelitian ini adalah untuk mengembangkan dan mengusulkan sebuah kerangka konseptual yang komprehensif yang memanfaatkan teknologi blockchain sebagai solusi inovatif dalam meningkatkan privasi dan kepercayaan pengguna di platform media sosial. Dengan demikian, penelitian ini bertujuan untuk mengidentifikasi dan menganalisis tantangan yang dihadapi dalam pengelolaan data pribadi, mengeksplorasi bagaimana penerapan blockchain dapat memberikan kontrol yang lebih besar kepada pengguna atas informasi mereka, dapat meningkatkan privasi, kepercayaan, dan keamanan dalam platform media sosial melalui penggunaan teknologi blockchain, dan mengurangi risiko penyalahgunaan data, sehingga dapat menciptakan lingkungan digital yang lebih aman dan terpercaya bagi semua pengguna serta meningkatkan pengalaman pengguna dan memastikan bahwa data pribadi mereka aman dan terlindungi.

2. METODOLOGI PENELITIAN



Gambar 1. Struktur Penelitian

Penelitian ini menggunakan pendekatan deskriptif kualitatif untuk mengeksplorasi dan menganalisis penerapan teknologi blockchain dalam meningkatkan privasi dan kepercayaan pengguna di platform media sosial. Metode ini dipilih karena memungkinkan peneliti untuk mendapatkan pemahaman yang mendalam tentang fenomena yang diteliti melalui pengumpulan data yang bersifat deskriptif.

a. Pengumpulan Data

1. Pengumpulan data dilakukan melalui beberapa teknik, antara lain:
2. Studi Pustaka: Peneliti melakukan analisis terhadap berbagai literatur, termasuk jurnal akademik, artikel, dan buku yang relevan dengan topik privasi, kepercayaan, dan teknologi blockchain. Ini bertujuan untuk membangun landasan teoritis yang kuat dan memahami konteks yang lebih luas dari penelitian ini.
3. Analisis Kasus: Penelitian ini juga mencakup studi kasus dari platform media sosial yang telah berhasil menerapkan teknologi blockchain. Melalui analisis ini, peneliti dapat mengidentifikasi praktik terbaik, tantangan yang dihadapi, serta dampak dari implementasi blockchain terhadap privasi dan kepercayaan pengguna.

b. Analisis Data

1. Data yang dikumpulkan akan dianalisis secara kualitatif dengan menggunakan teknik analisis tematik. Proses ini meliputi
2. Kategorisasi: Mengelompokkan data berdasarkan tema-tema utama yang muncul dari studi pustaka dan analisis kasus

3. Interpretasi: Menafsirkan hasil analisis untuk mengidentifikasi pola, hubungan, dan implikasi yang relevan terhadap tujuan penelitian.
- c. Validasi Data
 1. Untuk memastikan keakuratan dan kredibilitas data, peneliti akan melakukan triangulasi dengan membandingkan informasi dari berbagai sumber dan metode. Ini termasuk
 2. Cross-Referencing: Memverifikasi informasi dari studi pustaka dengan data yang diperoleh dari analisis kasus
 3. Diskusi dengan Ahli: Mengadakan wawancara atau diskusi dengan para ahli di bidang blockchain dan media sosial untuk mendapatkan perspektif tambahan dan validasi terhadap temuan penelitian.
- d. Etika Penelitian

Penelitian ini akan mematuhi prinsip-prinsip etika penelitian, termasuk mendapatkan izin dari sumber data yang digunakan dan menjaga kerahasiaan informasi yang sensitif. Peneliti juga akan memastikan bahwa semua partisipan dalam wawancara atau diskusi diberi penjelasan yang jelas tentang tujuan penelitian dan hak-hak mereka

3. HASIL DAN PEMBAHASAN

3.1 Tantangan Utama Privasi dan Kepercayaan dalam Media Sosial

Di zaman digital saat ini, media sosial menjadi bagian yang tak bisa terlepas dari kehidupan kita saat ini. Social media seperti Facebook, Instagram, Twitter, dan TikTok sangat memberikan berbagai manfaat, seperti kemudahan komunikasi, akses informasi, dan pembentukan komunitas. Namun, selain dari manfaatnya tersebut, media sosial tradisional sering kali dihadapkan pada berbagai tantangan yang mengkhawatirkan, terutama terkait privasi dan kepercayaan pengguna. Tantangan ini meliputi:

a. Pengumpulan Data yang Invasif

Platform media sosial tradisional mengumpulkan data pengguna dalam jumlah besar, termasuk informasi pribadi seperti profil, aktivitas online, dan interaksi dengan pengguna lain. Data ini sering kali dikumpulkan tanpa persetujuan eksplisit pengguna dan digunakan untuk berbagai tujuan, seperti periklanan bertarget, pengembangan produk, dan analisis perilaku pengguna. Pengguna mungkin tidak menyadari bagaimana data mereka digunakan dan untuk tujuan apa, dan hal ini dapat berakibat pada penargetan iklan yang invasif, profiling pengguna yang tidak akurat, dan bahkan penyalahgunaan data pribadi. Solusi potensial untuk mengatasi masalah ini adalah dengan memberikan kontrol data pengguna yang lebih kuat, transparansi data yang lebih besar, dan penerapan praktik privasi yang bertanggung jawab oleh platform media sosial.

b. Pelanggaran Privasi

Kasus kebocoran data dan penyalahgunaan data pribadi pengguna sering kali terjadi di platform media sosial tradisional. Hal ini dapat menyebabkan pencurian identitas, penipuan, dan kerugian finansial bagi pengguna. Pengguna mungkin kehilangan kontrol atas data pribadi mereka, reputasi dan peluang mereka dapat rusak, dan mereka bahkan dapat mengalami kerugian finansial akibat penyalahgunaan data. Peningkatan keamanan data, protokol pelaporan pelanggaran data yang jelas, dan kompensasi bagi pengguna yang terkena dampak kebocoran data atau penyalahgunaan data pribadi adalah solusi yang dapat membantu mengatasi pelanggaran privasi di media sosial.

c. Keamanan Platform

Platform media sosial harus aman dan terlindungi dari peretasan dan serangan lainnya. Penyalahgunaan platform untuk tujuan jahat, seperti penyebaran informasi yang salah, ujaran kebencian, dan konten berbahaya lainnya, dapat berakibat pada kerugian finansial, kerusakan reputasi, dan pembatasan peluang bagi pengguna. Peningkatan keamanan platform, moderasi konten yang lebih efektif, dan tata kelola platform yang baik adalah solusi yang dapat membantu meningkatkan keamanan dan kepercayaan pengguna terhadap platform media sosial. Secara keseluruhan, privasi dan kepercayaan merupakan faktor fundamental dalam penggunaan media sosial. Mengatasi berbagai tantangan yang terkait dengan privasi dan kepercayaan di media sosial sangat

penting untuk menciptakan lingkungan online yang aman, transparan, dan bertanggung jawab bagi semua pengguna.

3.2 Kontrol Privasi atas Data Pribadi

Privasi merupakan hak asasi setiap individu untuk melindungi informasi pribadi mereka. Dalam media sosial, privasi menjadi hal yang sangat penting untuk dijaga, karena platform ini mengumpulkan dan menyimpan data pengguna dalam jumlah besar. Konsep keamanan data memiliki tiga aspek utama, yaitu kerahasiaan, integritas, dan ketersediaan data. Kerahasiaan data berkaitan dengan pemeliharaan privasi data dari pihak yang tidak berhak mengaksesnya[12]. Pengguna media sosial memiliki hak untuk menentukan bagaimana data pribadi mereka dikumpulkan, digunakan, dan dibagikan. Terdapat beberapa aspek utama privasi di media sosial:

a. Kontrol Data: Pengguna harus memiliki kontrol atas data yang mereka bagikan di platform media sosial, dan bagaimana data tersebut digunakan. Hal ini meliputi:

1. Memilih data yang dibagikan: Pengguna harus dapat memilih jenis informasi yang mereka bagikan di platform, seperti informasi pribadi, demografi, dan aktivitas online.
2. Menentukan penggunaan data: Pengguna harus dapat menentukan bagaimana data mereka digunakan oleh platform media sosial, termasuk untuk tujuan periklanan, pengembangan produk, dan analisis perilaku.
3. Mengubah atau menghapus data: Pengguna memiliki hak untuk mengubah atau menghapus data mereka yang disimpan di platform media sosial.

b. Transparansi Data: Platform media sosial harus transparan tentang bagaimana mereka mengumpulkan, menggunakan, dan mengungkapkan data pengguna. Hal ini meliputi:

1. Metode pengumpulan data: Platform media sosial harus menjelaskan dengan jelas bagaimana mereka mengumpulkan data pengguna, termasuk jenis data yang dikumpulkan, sumber data, dan metode pengumpulan.
2. Penggunaan data: Platform media sosial harus menjelaskan dengan jelas bagaimana mereka menggunakan data pengguna, termasuk untuk tujuan apa data digunakan, dengan siapa data dibagikan, dan bagaimana data dianalisis.
3. Kebijakan privasi: Platform media sosial harus memiliki kebijakan privasi yang jelas dan mudah dipahami yang menjelaskan hak privasi pengguna dan bagaimana data mereka dilindungi.

c. Keamanan Data: Platform media sosial harus mengambil langkah-langkah yang tepat untuk melindungi data pengguna dari akses yang tidak sah, pencurian, dan penyalahgunaan. Hal ini meliputi:

1. Melindungi data dari akses yang tidak sah: Platform media sosial harus menerapkan langkah-langkah keamanan yang kuat untuk melindungi data pengguna dari akses yang tidak sah, termasuk peretasan, pencurian data, dan kebocoran data.
2. Mencegah penyalahgunaan data: Platform media sosial harus memiliki mekanisme untuk mencegah penyalahgunaan data pengguna, seperti penipuan, penargetan iklan yang invasif, dan profiling pengguna yang tidak akurat.
3. Memastikan kepatuhan terhadap peraturan privasi: Platform media sosial harus mematuhi semua peraturan privasi yang berlaku.

3.3 Kepercayaan pada Platform Media Sosial

Kepercayaan mengacu pada keyakinan individu bahwa platform media sosial akan bertindak dengan cara yang aman, bertanggung jawab, dan etis. Dalam konteks media sosial, kepercayaan mencakup beberapa aspek:

a. Keamanan Platform:

1. Sistem Keamanan yang Kuat

Platform media sosial harus menerapkan sistem keamanan yang kuat untuk melindungi data pengguna dari orang yang tidak bertanggung jawab, malware, dan pencurian data. Hal ini dapat dilakukan dengan menerapkan enkripsi data, autentikasi dua faktor, dan pemantauan aktivitas yang mencurigakan.

2. Perlindungan Privasi

Platform media sosial harus menghormati privasi pengguna dan mematuhi peraturan privasi yang berlaku, seperti UU PDP di Indonesia. Hal ini dapat dilakukan dengan menyediakan kontrol privasi yang terperinci, memberikan transparansi tentang penggunaan data pengguna, dan menerapkan kebijakan privasi yang jelas dan mudah dipahami.

3. Transparansi dan Akuntabilitas

Platform media sosial harus transparan tentang praktik keamanannya dan akuntabel kepada penggunanya atas pelanggaran keamanan. Hal ini dapat dilakukan dengan menerbitkan laporan transparansi keamanan, memberikan pemberitahuan kepada pengguna tentang pelanggaran data, dan menyediakan mekanisme bagi pengguna untuk melaporkan masalah keamanan.

b. Tata Kelola Platform

1. Kepemimpinan yang Bertanggung Jawab

Platform media sosial harus memiliki kepemimpinan yang bertanggung jawab dan berkomitmen untuk melindungi kepentingan pengguna. Hal ini dapat dilakukan dengan memastikan bahwa dewan direksi dan tim manajemen platform terdiri dari individu yang kompeten, berpengalaman, dan memiliki integritas tinggi.

2. Proses Pengambilan Keputusan yang Transparan

Platform media sosial harus memiliki proses pengambilan keputusan yang transparan dan melibatkan pengguna dalam keputusan yang berdampak pada mereka. Hal ini dapat dilakukan dengan mengadakan konsultasi publik, melakukan survei pengguna, dan memberikan mekanisme bagi pengguna untuk memberikan masukan tentang kebijakan dan praktik platform.

3. Akuntabilitas kepada Pemangku Kepentingan

Platform media sosial harus akuntabel kepada penggunanya, pemerintah, dan organisasi masyarakat sipil atas tindakan dan keputusannya. Hal ini dapat dilakukan dengan mematuhi hukum dan peraturan yang berlaku, bekerja sama dengan otoritas terkait untuk menyelidiki pelanggaran, dan menanggapi keluhan pengguna dengan serius.

c. Etika Platform:

Penggunaan Data yang Bertanggung Jawab: Platform media sosial harus menggunakan data pengguna dengan cara yang bertanggung jawab dan etis, dan tidak menyalahgunakan data untuk kepentingan pribadi atau komersial. Hal ini dapat dilakukan dengan membatasi pengumpulan data hanya pada data yang benar-benar diperlukan untuk menjalankan platform, memberikan kontrol privasi yang kuat kepada pengguna, dan menerapkan kebijakan penggunaan data yang transparan dan akuntabel. **Perlindungan dari Konten Berbahaya:** Platform media sosial harus mengambil langkah-langkah untuk melindungi penggunanya dari konten berbahaya, seperti ujaran kebencian, penindasan online, dan informasi yang salah. Hal ini dapat dilakukan dengan mengembangkan kebijakan konten yang jelas dan konsisten, menerapkan teknologi untuk mendeteksi dan menghapus konten berbahaya, dan bekerja sama dengan organisasi masyarakat sipil untuk memerangi penyalahgunaan platform.

d. Promosi Nilai-nilai Positif:

Platform media sosial harus mempromosikan nilai-nilai positif, seperti toleransi, inklusivitas, dan rasa hormat antar individu. Hal ini dapat dilakukan dengan mendukung komunitas positif di platform, mempromosikan dialog dan pemahaman antar pengguna, dan memberikan edukasi tentang penggunaan media sosial yang bertanggung jawab.

3.4 Teknologi Blockchain sebagai Solusi Desentralisasi dan Transparansi Digital

Teknologi blockchain merupakan teknologi desentralisasi yang memungkinkan pencatatan transaksi secara aman dan transparan. Blockchain terdiri dari jaringan komputer yang terdistribusi yang menyimpan buku besar publik dari semua transaksi. Transaksi dicatat dalam blok yang ditautkan satu sama lain, dan setiap blok diamankan dengan kriptografi yang kuat. Teknologi blockchain memiliki beberapa karakteristik yang membuatnya menarik untuk aplikasi dalam media sosial, diantaranya:

- a. **Desentralisasi:** Blockchain tidak dikendalikan oleh satu entitas tunggal, melainkan didistribusikan ke jaringan komputer yang luas. Hal ini memberikan kontrol dan transparansi yang lebih besar kepada pengguna atas data mereka.
- b. **Keamanan:** Blockchain menggunakan kriptografi yang kuat untuk mengamankan data dan transaksi, membuatnya tahan terhadap peretasan dan manipulasi.
- c. **Transparansi:** Semua transaksi di blockchain dicatat dalam buku besar publik yang dapat diakses oleh semua orang. Hal ini memungkinkan verifikasi dan audit yang mudah, meningkatkan akuntabilitas dan kepercayaan.

Dari karakteristik itu muncul pengembangan smart contract (smart contract menjadi populer karena kode-kodenya dimasukkan ke dalam buku besar blockchain), yaitu sebuah perjanjian antara dua orang dalam bentuk kode komputer dengan syarat dan ketentuan yang berada di jaringan blockchain[15].

3.5 Kerangka Konseptual: Mengintegrasikan Blockchain untuk Privasi dan Kepercayaan

Jurnal ini mengusulkan kerangka konseptual yang komprehensif untuk meningkatkan privasi dan kepercayaan dalam platform media sosial melalui teknologi blockchain. Kerangka ini didasarkan pada tinjauan literatur yang ekstensif dan analisis mendalam tentang tantangan privasi dan kepercayaan dalam media sosial, serta potensi solusi yang ditawarkan oleh teknologi blockchain. Kerangka ini mencakup dua pilar utama blockchain:

a. Kontrol Data Pengguna yang Lengkap: Memberdayakan Pengguna

Kontrol data pengguna yang lengkap, sebagai bagian dari upaya untuk memberdayakan pengguna, mengacu pada memberikan pengguna kekuatan dan kendali sepenuhnya atas informasi pribadi mereka yang dikumpulkan oleh platform media sosial. Berikut adalah penjelasan lebih rinci tentang bagaimana teknologi blockchain dapat digunakan untuk memberikan kontrol tersebut:

1. Akses yang Aman dan Transparan

Melalui penggunaan blockchain, pengguna diberikan akses yang aman dan transparan ke data mereka. Teknologi blockchain menawarkan keamanan yang tinggi melalui struktur data terdesentralisasi dan enkripsi kriptografis. Ini berarti bahwa data pengguna disimpan secara aman di dalam blockchain dan hanya dapat diakses oleh pemiliknya menggunakan kunci enkripsi yang tepat. Transparansi blockchain juga memungkinkan pengguna untuk melihat dan memahami bagaimana data mereka digunakan, siapa yang mengaksesnya, dan untuk tujuan apa. Dengan demikian, pengguna memiliki kendali penuh atas informasi pribadi mereka.

2. Hak Privasi yang Kuat

Blockchain memungkinkan pemberian hak privasi yang kuat kepada pengguna. Ini termasuk hak untuk menghapus data mereka dari platform, membatasi pengumpulan data yang dilakukan oleh platform, dan memilih cara bagaimana data mereka dapat digunakan, terutama untuk tujuan komersial. Melalui kontrak pintar (smart contracts) di blockchain, pengguna dapat menetapkan aturan dan batasan yang jelas tentang bagaimana data mereka dapat diakses dan digunakan oleh pihak lain. Ini memberikan pengguna kontrol yang lebih besar atas privasi mereka, serta memberikan mekanisme yang jelas untuk menegakkan hak-hak privasi mereka.

3. Portabilitas Data

Selain itu, blockchain memungkinkan portabilitas data, yang memungkinkan pengguna untuk dengan mudah mentransfer data mereka ke platform lain. Data yang disimpan di dalam blockchain bersifat portabel, karena blockchain adalah jaringan terdistribusi yang terbuka. Ini berarti bahwa pengguna dapat mengambil data mereka dari satu platform dan mentransferkannya ke platform lain tanpa hambatan yang signifikan. Hal ini memberikan pengguna lebih banyak pilihan dan kendali atas data mereka, serta mendorong persaingan sehat di antara platform-platform media sosial untuk memberikan layanan terbaik kepada pengguna mereka.

Dengan demikian, menggunakan teknologi blockchain untuk memberikan kontrol data pengguna yang lengkap membawa manfaat signifikan bagi pengguna, termasuk meningkatkan keamanan, privasi, dan portabilitas data mereka di lingkungan media sosial. **Konsensus dan Keaslian Data: Teknologi Blockchain menggunakan**

algoritma konsensus untuk memverifikasi dan mencapai kesepakatan antara berbagai node dalam jaringan. Hal ini memastikan bahwa data yang disimpan dalam blockchain adalah akurat dan asli. Jika ada percobaan manipulasi atau penyimpangan data, konsensus akan mengidentifikasinya[16].

b. Identitas Digital yang Aman dan Terverifikasi: Membangun Kepercayaan

Identitas digital yang aman dan terverifikasi menjadi kunci penting dalam membangun kepercayaan di platform media sosial. Berikut adalah penjelasan lebih rinci tentang bagaimana blockchain dapat digunakan untuk menciptakan identitas digital yang aman dan terverifikasi:

Keamanan Identitas: Blockchain dapat digunakan untuk menyimpan identitas digital pengguna dengan cara yang aman. Dalam konteks ini, informasi identitas seperti nama, alamat, dan data lainnya dapat dienkripsi dan disimpan dalam blok-blok yang terenkripsi di dalam blockchain. Karena sifatnya yang terdesentralisasi dan menggunakan teknologi enkripsi yang kuat, blockchain menyediakan tingkat keamanan yang tinggi terhadap upaya pencurian atau manipulasi data identitas.

Terverifikasi Melalui Kriptografi: Blockchain menggunakan kriptografi untuk memverifikasi identitas digital pengguna. Setiap entitas di dalam blockchain memiliki kunci publik dan kunci privat yang unik. Identitas pengguna dapat diverifikasi dengan cara memvalidasi tanda tangan digital yang dihasilkan menggunakan kunci privat mereka. Ini memungkinkan platform media sosial untuk memastikan bahwa identitas pengguna adalah sah dan terverifikasi tanpa harus mengungkapkan informasi identitas sebenarnya.

Immutabilitas dan Transparansi: Informasi identitas yang disimpan di dalam blockchain bersifat tidak dapat diubah (immutability) dan transparan. Ini berarti bahwa data identitas yang sudah diverifikasi tidak dapat dimodifikasi tanpa konsensus dari seluruh jaringan blockchain. Hal ini menciptakan tingkat kepercayaan yang tinggi karena memastikan bahwa informasi identitas yang disajikan oleh pengguna adalah valid dan tidak dapat dipalsukan.

Pengendalian Privasi oleh Pengguna: Dengan menggunakan blockchain, pengguna juga dapat memiliki lebih banyak kendali atas privasi identitas mereka. Mereka dapat memilih informasi identitas apa yang mereka ingin berbagi dengan platform media sosial dan dengan pengguna lainnya, serta menetapkan aturan-aturan terkait akses dan penggunaan informasi identitas mereka.

Dengan demikian, penggunaan blockchain untuk menciptakan identitas digital yang aman dan terverifikasi membantu membangun kepercayaan di platform media sosial dengan memastikan bahwa identitas pengguna valid, terlindungi, dan dapat diverifikasi secara kriptografis. Hal ini juga membuka potensi untuk membangun sistem yang lebih aman di lingkungan media sosial. Keunggulan blockchain sering dipergunakan untuk menutupi transaksi ilegal yang sering dilakukan oleh penjahat cyber, karna jaringan blockchain ini tempat yang aman dalam bertransaksi sebab sulitnya melacak identitas serta transaksi pada jaringan ini. Dalam pengimplementasiannya teknologi ini dapat digunakan sebagai dasar pembuatan berbagai macam platform. Salah satu hal yang dapat dilakukan adalah pembuatan mata uang digital yang lebih dikenal dengan cryptocurrency[17].

3.6 Kekurangan dan Resiko Penggunaan Teknologi Blockchain

Penggunaan teknologi blockchain juga memiliki beberapa risiko, seperti ketergantungan pada teknologi, risiko keamanan, dan keterbatasan skalabilitas. Jika teknologi blockchain mengalami masalah atau kegagalan, maka data dan transaksi yang disimpan dalam blockchain juga akan terkena dampaknya. Selain itu, masalah keamanan juga merupakan risiko utama dalam penggunaan teknologi blockchain untuk keamanan data. Meskipun teknologi blockchain dianggap sangat aman, namun tidak menutup kemungkinan adanya serangan yang berhasil menembus sistem keamanannya. Dalam jaringan blockchain terdapat beberapa jenis serangan yang dapat terjadi seperti serangan 51% attack yang terjadi ketika penyerang berhasil menguasai lebih dari 50% kekuatan jaringan blockchain dan penyerang dapat memalsukan transaksi dan mengganti catatan transaksi yang telah dilakukan sebelumnya (hal itu dapat merusak integritas data dan mengancam keamanan data blockchain), double-spending attack merupakan serangan yang di mana seorang penyerang itu mencoba untuk melakukan transaksi yang sama dua kali menggunakan aset kripto yang sama, sybil attack dan lain-lain[12]. Teknologi ini memiliki potensi untuk dapat menanggulangi berbagai serangan[18]. Penggunaan teknologi

Blockchain juga bisa disalah gunakan oleh orang yang tidak bertanggung jawab, seperti melakukan transaksi ilegal dan menggunakan teknologi Blockchain membutuhkan biaya yang mahal, dikarenakan dalam membuat teknologi ini hanya bisa dilakukan oleh orang yang ahli saja, dan kurangnya tenaga yang ahli membuat teknologi ini cukup menguras biaya[3].

3.7 Implementasi

Implementasi teknologi blockchain di Indonesia memiliki beberapa tantangan, seperti regulasi yang belum jelas, infrastruktur nya yang masih terbatas, dan kurangnya pemahaman tentang teknologi blockchain. Oleh karena itu, diperlukan dukungan dari semua pihak untuk mempercepat adopsi teknologi blockchain di Indonesia. Untuk mengoptimalkan potensi teknologi blockchain dan mempercepat transformasi digital di Indonesia harus dilakukan penelitian yang lebih lanjut[12]. Implementasi blockchain dalam media sosial dapat memberikan pengguna kontrol penuh atas data mereka, membangun identitas digital yang aman, dan meningkatkan transparansi dalam pengambilan keputusan dan operasi platform. Diharapkan jurnal ini dapat memberikan kontribusi dalam memahami serta mengatasi tantangan privasi dan kepercayaan dalam media sosial, serta menjadi panduan penting bagi para pemangku kepentingan dalam mengembangkan platform media sosial yang lebih aman, transparan, dan berpusat pada pengguna.

Teknologi blockchain dapat diimplementasikan dalam media sosial untuk mengatasi berbagai tantangan privasi dan kepercayaan. Berikut beberapa contoh implementasi blockchain dalam media sosial meliputi:

Steemit: Steemit merupakan platform media sosial berbasis blockchain yang memiliki cara kerja pengguna steemit untuk memposting konten, memberikan suara, dan pengguna akan mendapatkan imbalan dalam bentuk koin kripto STEEM. Pengguna dapat menghasilkan pendapatan dari konten yang mereka buat, berdasarkan interaksi dan nilai yang diberikan oleh komunitas.

Verifikasi Identitas: Verifikasi Identitas merupakan fitur pada platform social media yang memanfaatkan teknologi blockchain, untuk memudahkan seorang individu membuktikan identitas mereka secara daring online dengan aman dan mudah[19].

Sapien Network: Sapien Network merupakan platform media sosial yang memanfaatkan blockchain untuk memberdayakan pengguna dengan kontrol penuh atas privasi dan keamanan data mereka. Sapien Network memberikan imbalan berbasis cryptocurrency (SPN) kepada pengguna yang sudah berkontribusi dalam komunitas.

4. KESIMPULAN

Salah satu solusi dalam meningkatkan keamanan data dalam era digital saat ini ialah Teknologi Blockchain. Sistem yang terdesentralisasi dalam blockchain, tidak dapat dimanipulasi dan sistem pada blockchain ini dapat digunakan untuk menciptakan catatan transaksi yang aman serta transparan. Dalam era di mana media sosial telah menjadi bagian integral dari kehidupan modern, tantangan privasi dan kepercayaan pengguna menjadi semakin penting untuk diatasi. Melalui penggunaan teknologi blockchain, jurnal ini telah mengusulkan sebuah kerangka konseptual yang komprehensif untuk meningkatkan privasi dan kepercayaan dalam platform media sosial. Dari tinjauan literatur yang mendalam, ditemukan bahwa blockchain dapat memberikan solusi yang signifikan terhadap masalah pengumpulan data yang invasif, keamanan informasi, dan transparansi dalam pengelolaan data pengguna. Dengan membangun kontrol data pengguna yang lengkap, identitas digital yang aman dan terverifikasi, serta tata kelola platform yang transparan dan akuntabel, implementasi blockchain diharapkan bisa memberikan pengguna kontrol penuh atas data mereka pribadi, membangun identitas digital yang aman, dan meningkatkan transparansi dalam pengambilan keputusan dan operasi platform. Dengan memanfaatkan teknologi blockchain dalam platform media sosial, dapat membantu untuk meningkatkan privasi dan kepercayaan masyarakat sebab data yang mereka miliki lebih aman dan juga transparan. Bisa kita lihat bersama, tinggi nya tingkat kejahatan pada era digital saat ini seperti manipulasi data yang merugikan individu maupun kelompok, dengan hal itu penting nya untuk setiap individu meningkatkan keamanan data pribadi. Diharapkan bahwa jurnal ini dapat memberikan kontribusi dalam memahami dan mengatasi tantangan privasi dan kepercayaan dalam media sosial. Sebagai panduan penting bagi para pemangku kepentingan, implementasi blockchain diharapkan dapat membawa perubahan positif dalam mengembangkan platform media sosial yang lebih aman, transparan, dan berpusat pada pengguna.

REFERENCES

- [1] M. H. A. Pakarti, D. Farid, H. Hendriana, U. Saepullah, and I. Sucipto, "Pengaruh perkembangan teknologi terhadap perlindungan privasi dalam hukum perdata," *Sultan Adam J. Huk. dan Sos.*, vol. 1, no. 1, p. hal 2, 2023.
- [2] N. P. A., "Memahami Dan Meengelola Transformasi Digital," *Trakia J. Sci.*, vol. 15, no. Suppl.1, pp. 388–393, 2017, doi: 10.15547/tjs.2017.s.01.065.
- [3] 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, 2024, doi: 10.59024/jise.v2i2.653.
- [4] Iswanto, N. I. Putri, Z. Munawar, R. Komalasari, and Dandun Widhiantoro, "Analisis Pemanfaatan Teknologi Blockchain di Bidang Pendidikan," *Tematik*, vol. 9, no. 2, pp. 174–181, 2022, doi: 10.38204/tematik.v9i2.1082.
- [5] M. Yusup, Q. Aini, D. Apriani, and P. Nursaputri, "Pemanfaatan teknologi blockchain pada program sertifikasi dosen 1,2,3," *Semin. Nas. Sist. Inf. dan Tek. Inform.*, pp. 365–371, 2019.
- [6] P. A., "Penggunaan Teknologi Blockchain Dalam Upaya Meningkatkan Keamanan Data Di Massa Era Digital," no. April, pp. 1–11, 2023, [Online]. Available: <https://www.researchgate.net/publication/370074662>
- [7] T. P. Utomo, "Implementasi Teknologi Blockchain Di Perpustakaan: Peluang, Tantangan Dan Hambatan," *Bul. Perpust.*, vol. 4, no. 2, pp. 173–200, 2022.
- [8] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117–2135, 2019, doi: 10.1080/00207543.2018.1533261.
- [9] I. Abunadi and R. L. Kumar, "Bsf-ehr: Blockchain security framework for electronic health records of patients," *Sensors*, vol. 21, no. 8, pp. 1–10, 2021, doi: 10.3390/s21082865.
- [10] J. J. Bambara and R. A. Paul, "Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions," Ohio McGraw-Hill Educ., 2018.
- [11] P. H. Eka, A. Qurotul, and K. A. Reza, "Pemanfaatan Teknologi Blockchain Pada Platform," vol. 4, no. 2, 2020.
- [12] T. W. E. Suryawijaya, "Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia," *J. Stud. Kebijak. Publik*, vol. 2, no. 1, pp. 55–68, 2023, doi: 10.21787/jskp.2.2023.55-68.
- [13] A. Rizky, W. Athoilah, M. Zarkasih, and ..., "Implementasi Teknologi Blockchain Untuk Optimalisasi Keamanan Pengarsipan Surat Masuk dan Keluar Pada Sebuah Perusahaan," ... *Educ. Sains ...*, vol. 5, no. 2, pp. 452–457, 2022, [Online]. Available: <https://jurnal.uisu.ac.id/index.php/best/article/view/6058%0Ahttps://jurnal.uisu.ac.id/index.php/best/article/download/6058/4939>
- [14] R. K. Novriantama, A. Kusyanti, and R. I. Rokhmawati, "Analisis Privasi dan Kepercayaan Terhadap Keamanan Data Pengguna Aplikasi On Demand Service Menggunakan Metodologi Structural Equation Modeling," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 3, pp. 1161–1169, 2018.
- [15] A. Fachmi and N. Mayesti, "Tinjauan literatur argumentatif tentang kepemilikan data arsip digital non-fungible token (NFT) pada teknologi blockchain," *Berk. Ilmu Perpust. dan Inf.*, vol. 18, no. 1, pp. 144–158, 2022, doi: 10.22146/bip.v18i1.3989.
- [16] I. Kamaruddin, S. Surya, and M. R. Tawil, "Masalah Kesehatan Dan Data Dalam Teknologi," vol. 8, pp. 847–853, 2024.
- [17] Bisma Adjie Trisna Yahya, "Mitigasi Risiko Teknologi Blockchain Dalam Transaksi Cryptocurrency (Studi Kasus Pada Bitcoin)," *Pap. Knowl. . Towar. a Media Hist. Doc.*, pp. 1–12, 2014.
- [18] I. Riadi, R. Umar, and I. Busthomi, "Optimasi Keamanan Autentikasi dari Man in the Middle Attack (MiTM) Menggunakan Teknologi Blockchain," *J. Inf. Eng. Educ. Technol.*, vol. 4, no. 1, pp. 15–19, 2020, doi: 10.26740/jieet.v4n1.p15-19.
- [19] E. P. Hendraswara et al., "Teknologi Blockchain Dan Potensi Pemanfaatannya Di Indonesia 2023," *Pokja PANDI*, pp. 1–87, 2023