Nusantara Journal of Multidisciplinary Science
Vol. 2, No. 4, November 2024
Hal 834-847
E-ISSN : 3024-8752
P-ISSN : 3024-8744
Site : https://jurnal.intekom.id/index.php/njms

Mengeksplorasi Teknologi *Blockchain:* Konsensus, Keamanan, Dan Implementasi

Joosten[1], Vanessa Taisri[2], Felicia Cenora[3], Siti Maharani Nur Fitria[4], Ricardo[5], Sony Wang[6], Devincent[7]
[1,2,3,4,5,6,7]Fakultas Informatika, Universitas Mikroskil, Medan, Indonesia

Article Info

Article history:

Received November 9, 2024
Revised November 9, 2024
Accepted November 10, 2024

Kata Kunci:

Blockchain,
Desentralisasi,
Konsensus

Keywords:

Blockchain,
Decentralization,
Consensus

ABSTRAK

Blockchain berfungsi sebagai buku besar digital yang terdesentralisasi, yang memungkinkan pencatatan transaksi secara aman tanpa memerlukan perantara. Berbagai mekanisme konsensus, seperti Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), dan Delegated Proof of Stake (DPoS), memiliki peran krusial dalam menjaga integritas data. PoW dikenal karena tingkat keamanannya yang tinggi, meskipun mengonsumsi energi secara berlebihan, sedangkan PoS menawarkan solusi yang lebih efisien dalam hal penggunaan energi. PBFT dan DPoS lebih menekankan pada kecepatan dan efisiensi, sehingga lebih sesuai untuk aplikasi tertentu. Namun, teknologi ini juga menghadapi tantangan, termasuk ketergantungan pada teknologi, risiko keamanan seperti serangan 51%, dan masalah skalabilitas. Dengan pengelolaan risiko yang tepat, blockchain memiliki potensi untuk mendukung transformasi digital yang berkelanjutan di berbagai industri. Oleh karena itu, kolaborasi antara pemerintah, sektor industri, dan komunitas teknologi sangat diperlukan untuk menciptakan regulasi yang mendukung serta lingkungan inovasi yang adaptif.

ABSTRACT

Blockchain functions as a decentralized digital ledger, which allows for secure recording of transactions without the need for intermediaries. Various consensus mechanisms, such as Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Delegated Proof of Stake (DPoS), play a crucial role in maintaining data integrity. PoW is known for its high level of security, although it consumes excessive energy, while PoS offers a more efficient solution in terms of energy usage. PBFT and DPoS emphasize speed and efficiency, making them more suitable for certain applications. However, this technology also faces challenges, including technology dependence, security risks such as 51% attacks, and scalability issues. With proper risk management, blockchain has the potential to support the ongoing digital transformation of various industries. Therefore, collaboration between the government, industrial sector, and technology community is essential to create supportive regulations and an adaptive innovation environment.

Corresponding Author:

Joosten
Fakultas Informatika, Universitas Mikroskil,
Medan, Indonesia
Email: ricardo221103@gmail.com

1. PENDAHULUAN

Dunia teknologi semakin populer dan berkembang pesat di Indonesia, termasuk dalam bidang blockchain. Bermula dari keingintahuan masyarakat terhadap dunia cryptocurrency semakin tinggi, pencarian terhadap teknologi blockchain juga sangat marak bukan hanya pada kalangan IT saja namun sampai menjadi sorotan bagi kalangan masyarakat yang umum sekalipun. Blockchain merupakan teknologi yang digunakan sebagai sistem penyimpanan atau bank data secara digital yang terhubung dengan kriptografi [1]. Blockchain adalah struktur data terdistribusi yang terdiri dari blok rantai, bisa berupa buku besar global yang menyimpan catatan semua transaksi di jaringan blockchain. Dengan adopsi bitcoin yang cepat dan meluas, blockchain dipuji sebagai inovasi dalam paradigma komputasi [2]. Teknologi blockchain memiliki potensi besar dengan beragam aplikasi dan memberikan peluang luas untuk berbagai infrastruktur. Teknologi ini mendorong manajemen sumber daya dan membuat komunikasi menjadi aman dan efisien. Kepercayaan meningkat saat melakukan transaksi keuangan antar pihak menggunakan blockchain, karena mengurangi kemungkinan penipuan dan secara otomatis menghasilkan catatan aktivitas. Blockchain merupakan paradigma komputasi baru yang aman dan bermanfaat untuk mendukung inovasi bisnis [3].

Teknologi blockchain dapat menjadikan suatu transaksi lebih cepat, murah, transparan, dan aman. Bahkan dalam Kajian World Bank (2019) sistem blockchain adalah inovasi teknologi yang berpotensi memicu terjadinya revolusi industri yang akan mendisrupsi model ekonomi dan bisnis [2]. Dalam beberapa tahun terakhir, kepopuleran blockchain semakin meningkat seiring dengan tingginya minat masyarakat terhadap dunia cryptocurrency. Namun, teknologi blockchain tidak hanya berhubungan dengan cryptocurrency, tetapi juga memiliki potensi besar untuk mengubah dunia bisnis digital secara keseluruhan [1].

Bisa disimpulkan blockchain merupakan sebuah database yang tidak bisa diganti dan diubah karena teknologi ini menyimpan data digital yang terhubung dengan kriptografi. Teknologi ini membuat transaksi menjadi lebih transparan dan aman, yang dapat meminimalisir kecurangan dalam data keuangan. Sehingga, teknologi ini kemudian dimanfaatkan sebagai peluang dalam sektor utama di berbagai bidang bisnis digital seperti pada bidang keuangan atau finansial, bidang logistik, bidang kesehatan dan keamanan data, pemasaran dan iklan, media dan hiburan [4].

Pada sektor keuangan, teknologi ini dianggap sebagai laporan kas digital yang bisa diakses oleh siapa saja, kapan saja, di mana saja dengan mudah tanpa harus mendapatkan persetujuan dari pihak perantara seperti lembaga keuangan. Pada sektor logistik, teknologi blockchain ini dapat meningkatkan transparansi dan keamanan data. Dengan adanya teknologi ini, informasi yang diterima menjadi lebih jelas dan terintegrasi, di mana informasi mengenai asal usul produk, proses produksi, dan ketersediaan stok dapat dicatat secara terperinci dan dapat diakses oleh semua pihak yang berkepentingan. Hal ini meminimalisir adanya resiko pemalsuan produk, meningkatkan efisiensi operasional, kepercayaan konsumen terhadap

produk yang dibeli. Pada sektor kesehatan dan keamanan data, biasanya teknologi ini digunakan untuk menyimpan semua data medis dari pasien. Sehingga data medis pasien ini dapat diakses secara mudah dan aman oleh pihak yang berwenang dan menghindari penyalahgunaan data. Pada bidang pemasaran dan iklan, umumnya digunakan untuk meningkatkan transparansi yang mencegah penipuan serta memberikan imbalan bagi pengguna dengan adil dan akurat. Hal ini akan mengurangi resiko kecurangan dan memastikan bahwa pengiklan mendapatkan nilai yang sebanding dengan biaya iklan yang mereka keluarkan. Pada bidang media dan hiburan, digunakan untuk melindungi hak kekayaan intelektual, memastikan pembagian royalty yang adil bagi para pencipta konten, dan meningkatkan transparansi pada distribusi konten [1].

Dengan menguasai lebih dari 50% kekuatan jaringan, penyerang dapat memalsukan transaksi dan mengganti catatan transaksi yang telah dilakukan sebelumnya. Hal ini dapat merusak integritas data dan mengancam keamanan data dalam blockchain. Double-spending attack adalah serangan di mana seorang penyerang mencoba untuk melakukan transaksi yang sama dua kali menggunakan aset kripto yang sama. Dalam blockchain, setiap transaksi harus diverifikasi dan disetujui oleh seluruh jaringan. Namun, dalam doublespending attack, penyerang mencoba untuk memalsukan transaksi dan mengirimkan aset kripto yang sama ke dua alamat yang berbeda secara bersamaan. Hal ini dapat mengakibatkan kerugian finansial yang signifikan bagi pihak yang menerima aset kripto tersebut. Sybil attack adalah serangan di mana seorang penyerang mencoba untuk mengambil alih jaringan blockchain dengan membuat banyak identitas palsu. Dalam sybil attack, penyerang membuat banyak identitas palsu yang tampaknya berasal dari banyak node jaringan yang berbeda. Hal ini dapat membuat penyerang memiliki kekuatan yang lebih besar dalam jaringan dan dapat memalsukan transaksi dan data [5].

2. METODE

Penelitian ini dilakukan dengan menggunakan metode Systematic Literature Review (SLR). Systematic Literature Review (SLR) adalah sebuah metode penelitian yang merangkum hasil-hasil penelitian primer untuk menyajikan fakta yang lebih komprehensif. SLR dipilih sebagai metode penelitian karena memberikan kerangka kerja yang terstruktur untuk mengumpulkan informasi dari berbagai sumber terpercaya guna memahami aspek mekanisme konsensus, keamanan, dan penerapan teknologi blockchain di berbagai sektor. Dalam pelaksanaannya, SLR melibatkan serangkaian langkah yang dirancang untuk memastikan akurasi dan relevansi dari setiap temuan yang dikumpulkan.

Proses ini dimulai dengan mengidentifikasi pertanyaan penelitian, yang bertujuan untuk mentransformasi permasalahan kesehatan menjadi bentuk pertanyaan yang dapat diteliti. Langkah selanjutnya adalah mengembangkan protokol penelitian yang berfungsi sebagai panduan dalam menjalankan proses review secara sistematis. Setelah itu, dilakukan penetapan lokasi database hasil penelitian, seperti MEDLINE, PubMed, Google Scholar, IEEE Xplore, dan Scopus, sebagai wilayah pencarian. Pencarian difokuskan pada artikel-artikel yang membahas aspek teknis dan implementasi blockchain, khususnya yang diterbitkan dalam lima tahun terakhir. Dengan kata kunci seperti “blockchain consensus mechanisms”, “blockchain security” dan “blockchain application sectors” akan diperoleh artikel yang relevan dengan topik penelitian ini.

Setelah pencarian literatur, diterapkan kriteria inklusi dan eksklusi untuk menyaring artikel yang memenuhi standar kualitas dan relevansi. Artikel yang diterbitkan dalam jurnal bereputasi, berbahasa Inggris, dan berfokus pada mekanisme konsensus, keamanan, serta implementasi blockchain di berbagai sektor industri dipilih untuk dianalisis, sementara artikel yang tidak relevan atau tidak memenuhi kriteria kualitas dikeluarkan dari daftar literatur. Langkah berikutnya adalah pengumpulan data dari artikel yang telah diseleksi, di mana setiap artikel dianalisis untuk mengekstraksi informasi utama terkait teknologi konsensus yang digunakan, tantangan keamanan, serta sektor-sektor yang menerapkan blockchain. Data yang diperoleh dikelompokkan berdasarkan tema yang relevan, memudahkan analisis lebih lanjut.

Pada tahap analisis dan sintesis data, data yang terkumpul dianalisis untuk mengidentifikasi pola-pola, tren, dan kesimpulan umum di berbagai penelitian terkait. Analisis ini mencakup perbandingan berbagai mekanisme konsensus, identifikasi tantangan keamanan yang umum, serta evaluasi efektivitas implementasi blockchain di sektor tertentu. Synthesis dilakukan dengan merangkum temuan dari berbagai studi untuk menyusun kesimpulan komprehensif mengenai potensi, tantangan, dan aplikasi praktis blockchain dalam mendukung efisiensi, inovasi, serta keamanan data. Untuk menjaga validitas temuan, dilakukan verifikasi data antar-sumber, memastikan bahwa setiap kesimpulan sesuai dengan hasil studi lain dan mencerminkan kondisi serta potensi blockchain saat ini. Lalu, akhiri dengan kesimpulan singkat mengenai temuan yang paling signifikan dari keseluruhan penelitian yang direview [6].

3. HASIL DAN PEMBAHASAN

Blockchain diperkenalkan sebagai bagian dari sistem *Bitcoin* oleh Satoshi Nakamoto pada tahun 2008. Terdiri dari serangkaian blok yang berisi informasi, yang terhubung satu sama lain dan dilindungi dengan kriptografi. Setiap blok berisi data transaksi, timestamp, dan hash dari blok sebelumnya, menciptakan rantai yang tidak dapat diubah [7].

Teknologi ini memungkinkan pencatatan dan verifikasi transaksi secara aman tanpa memerlukan pihak ketiga. Landasan konseptual untuk teknologi *blockchain* muncul pada tahun 1991 ketika para peneliti Stuart Haber dan W. Scott Stornetta mengusulkan solusi yang dapat dihitung secara komputasional untuk penanda waktu dokumen digital, memastikan kekekalan dokumen tersebut. Sistem mereka menggunakan rantai blok yang aman secara kriptografis yang kemudian ditingkatkan pada tahun 1992 dengan integrasi pohon Merkle, meningkatkan efisiensi dengan menggabungkan beberapa dokumen menjadi satu blok. Meskipun inovasi ini, teknologi tersebut tetap tidak aktif, dan patennya kedaluwarsa pada tahun 2004, sebelum lahirnya *bitcoin* [9]. Pada 2008, *blockchain* pertama kali muncul dalam *whitepaper Bitcoin*. Nakamoto menjelaskan cara kerja *bitcoin* yang memanfaatkan *blockchain* untuk menciptakan sistem pembayaran *peer-to-peer* yang aman dan transparan. Teknologi ini memecahkan masalah double spending, di mana satu unit mata uang digital dapat dibelanjakan lebih dari sekali [8].

Pada 3 Januari 2009, blok *bitcoin* pertama ditambang, menandai lahirnya *bitcoin*. Penerima pertama, Hal Finney, berpartisipasi dalam transaksi *bitcoin* pertama pada 12 Januari 2009. Pada tahun 2013, Vitalik Buterin, salah satu pendiri *Bitcoin Magazine*, mengusulkan *ethereum*, *platform blockchain* yang memungkinkan pengembangan aplikasi terdesentralisasi (dApps) menggunakan *smart contracts* [10]. Ether, mata uang kripto asli *ethereum*,

memfasilitasi transaksi dan berfungsi sebagai pembayaran untuk daya komputasi yang digunakan saat mengeksekusi *smart contracts*. *Ethereum* diluncurkan, memperluas potensi *blockchain* di luar sekadar *cryptocurrency*. *Hyperledger* merupakan proyek *blockchain* terbuka yang dikembangkan oleh *Linux Foundation* pada 2015. Proyek ini bertujuan untuk mengembangkan teknologi *blockchain* yang dapat digunakan di berbagai sektor, seperti keuangan, kesehatan, dan logistik. DeFi (*Decentralized Finance*) adalah aplikasi keuangan yang memanfaatkan teknologi *blockchain* untuk memungkinkan pengguna melakukan transaksi keuangan secara terdesentralisasi. DeFi berkembang pesat pada tahun 2018, dengan jumlah pengguna dan aplikasi yang semakin meningkat [11].

3.1 Model Konsensus Pada *Blockchain*

Dalam teknologi *blockchain*, mekanisme konsensus berfungsi untuk mengatasi masalah skalabilitas sistem. Berbagai mekanisme konsensus memungkinkan node yang ada untuk memvalidasi transaksi dan menghasilkan blok baru. Model konsensus *blockchain* mencakup struktur dan cara kerja mekanisme konsensus tersebut, di mana setiap mekanisme berkontribusi pada kolaborasi antara node untuk mencapai kesepakatan[12]. Model konsensus terdiri dari:

A. *Proof of Work* (PoW)

Proof of Work (PoW) adalah sebuah model konsensus dalam blockchain di mana mekanismenya mencakup transaksi-transaksi dikumpulkan menjadi satu kelompok yang disebut blok. *Miners* bertugas untuk memverifikasi transaksi yang terdapat dalam setiap blok tersebut. Mereka harus memecahkan sebuah teka-teki matematika untuk menerima imbalan berupa aset kripto. Mekanisme ini membutuhkan daya komputasi yang besar. Semakin tinggi kekuatan pemrosesan yang dimiliki oleh *Miner*, semakin besar peluang mereka untuk memecahkan teka-teki matematika tersebut lebih cepat daripada *Miner* lainnya. Karena tingginya persaingan dalam memecahkan teka-teki ini, *Miners* sering kali membentuk kumpulan atau *mining pool*. Dalam *mining pool*, *Miners* menggabungkan kekuatan komputasi mereka untuk meningkatkan peluang mereka dalam menyelesaikan blok. Hasil dari upaya ini dibagi secara proporsional sesuai dengan kontribusi kekuatan komputasi masing-masing *Miner*.

Mekanisme konsensus *Proof of Work* (PoW) memiliki beberapa kelemahan. Salah satunya adalah "*The 51% Attack"* atau serangan 51%, di mana jika suatu node atau sekelompok node menguasai 51% atau lebih dari kekuatan jaringan, mereka dapat memengaruhi dan mengontrol *blockchain*. Selain itu, PoW memerlukan waktu yang cukup lama dan daya yang sangat besar untuk menyelesaikan teka-teki kriptografi (*nonce)*.

B. *Proof of Stake* (PoS)

Proof of Stake (PoS) adalah sebuah model konsensus di mana mekanismenya terdiri dari transaksi-transaksi dikumpulkan menjadi satu kelompok yang disebut blok. Para validator akan mempertaruhkan (*stake*) sejumlah aset kripto mereka untuk berkesempatan dipilih secara acak melalui proses yang deterministik. Validator yang terpilih kemudian bertugas untuk membuat blok baru dan memvalidasi transaksi yang ada di dalamnya. validator akan menerima biaya transaksi dari blok yang berhasil mereka validasi.

Namun, jika seorang validator memverifikasi transaksi yang curang atau tidak sah, mereka akan kehilangan sebagian dari aset yang mereka pertaruhkan. Transaksi yang telah

diverifikasi kemudian disimpan dalam *blockchain* publik, yang memastikan transparansi dan keamanan data. Mekanisme PoS tidak bergantung pada kepercayaan (*trustless*), sehingga menjaga keamanan jaringan tanpa membutuhkan daya komputasi yang besar seperti pada Proof of Work (PoW).

Peralihan dari PoW ke PoS memiliki beberapa keuntungan, seperti penghematan energi dan keamanan jaringan yang lebih baik sehingga menciptakan jaringan yang lebih aman dan ramah lingkungan dibandingkan dengan PoW [13].

C. *Practical Byzantine Fault Tolerance* (PBFT)

Practical Byzantine Fault Tolerance (PBFT) pertama kali diperkenalkan oleh *Miguel Castro* dan *Barbara Liskov* pada tahun 1999, dengan tujuan untuk menyelesaikan masalah *Byzantine* secara lebih efisien. Model konsensus ini berhasil mengurangi kompleksitas waktu dari tingkat eksponensial menjadi tingkat polinomial.

Konsep inti dari PBFT terdiri atas tiga komponen utama, yaitu *view*, *replica*, dan *role*. Pandangan mencerminkan status global dari sistem saat ini, di mana setiap node yang berpartisipasi menjadi replika. Dalam setiap pandangan, satu replika bertindak sebagai *primary* (utama) dan yang lainnya sebagai *backups* (cadangan). Protokol model konsensus PBFT mencakup tiga aspek: protokol konsistensi, protokol penggantian pandangan, dan protokol *checkpoint*. Protokol konsistensi memastikan bahwa data yang disimpan oleh semua node dalam jaringan tetap konsisten melalui komunikasi antar-node dalam tiga tahap. Protokol penggantian pandangan digunakan untuk mengganti node yang bermasalah agar sistem tetap beroperasi dengan normal. Protokol *checkpoint* membantu mengurangi tekanan penyimpanan pada node dengan membersihkan data interaktif yang kedaluwarsa, memeriksa kesatuan sistem secara berkala, dan menyinkronkan node yang tidak konsisten. Protokol model konsensus ini terdiri dari tiga proses utama yang memastikan bahwa semua node dalam jaringan mencapai kesepakatan mengenai status transaksi sebelum data ditulis ke dalam *blockchain*, sehingga menjaga integritas dan konsistensi sistem.

i. *Pre-prepare*

Setelah node utama menerima pesan permintaan layanan dan memverifikasinya, node tersebut akan membuat pesan *pre-prepare* berdasarkan permintaan layanan tersebut, kemudian menyiarkan pesan tersebut ke node-node cadangan.

ii. *Prepare*

Node cadangan memverifikasi apakah isi pesan telah dimodifikasi atau tidak. Jika verifikasi berhasil, node cadangan akan membuat pesan *prepare* berdasarkan pesan *pre-prepare* dan menyiarkannya ke semua node replika.

iii. *Commit*

Node-node akan menyiarkan pesan *commit* kepada node lainnya. Setelah menerima $2f + 1$ pesan *commit* (termasuk dari dirinya sendiri), konsensus dianggap telah tercapai, dan node-node akan menjalankan permintaan tersebut serta menuliskan data ke sistem [14].

D. *Delegated Proof of Stake* (DPoS)

Delegated Proof of Stake (DPoS) adalah sebuah peningkatan lebih lanjut dari *Proof of Work* (PoW) dan *Proof of Stake* (PoS), dan merupakan model konsensus yang berbasis pada pemilihan melalui *voting*. Sejumlah wakil dipilih oleh pemegang mata uang untuk menjalankan kekuasaan atas nama mereka. Para wakil yang terpilih berpartisipasi dalam

konsensus dan secara bergiliran menghasilkan blok. Jika ada wakil yang tidak kompeten, pemilih dapat memberikan suara untuk mengeluarkannya dari jabatan. Meskipun DPoS secara signifikan meningkatkan throughput dan mengurangi latensi, terdapat beberapa masalah seperti rendahnya antusiasme dari node yang memberikan suara dan ketidakmampuan untuk menangani node jahat dengan cepat.

DPoS memiliki keuntungan dalam aksesibilitas dan skalabilitas. DPoS memungkinkan siapa saja yang memiliki token asli untuk berpartisipasi dalam proses pemungutan suara dan menjadi delegasi. DPoS dapat mencapai konsensus lebih cepat, dengan membatasi jumlah delegasi yang bertanggung jawab, yang mengarah pada throughput transaksi yang lebih tinggi dan peningkatan kinerja jaringan. DPoS tidak memerlukan konsumsi energi yang besar seperti pada sistem PoW.

Proses pemungutan suara yang berkelanjutan memastikan bahwa delegasi tetap akuntabel kepada komunitas, dan para pemangku kepentingan dapat berpartisipasi aktif dalam proses pengambilan keputusan. Struktur pemerintahan yang dinamis ini memungkinkan adaptasi dan implementasi perbaikan jaringan dengan cepat, sehingga meningkatkan ketahanan dan evolusi keseluruhan dari *blockchain*. Dalam model konsensus DPoS, pemegang mata uang memberikan suara untuk sejumlah wakil yang akan menjalankan kekuasaan atas nama mereka. Node *proxy* yang terpilih kemudian berpartisipasi dalam konsensus dan secara bergiliran menghasilkan blok. Jika sebuah node melakukan tindakan buruk, pemilih dapat mencabut kepercayaan terhadapnya melalui pemungutan suara.

Untuk mengatasi masalah ini, skema *Reputation*-DPoS menggunakan nilai reputasi node sebagai bobot referensi untuk memilih node delegasi. Kami memilih sejumlah node delegasi berdasarkan hasil *voting* dan nilai reputasi. Selain itu, nilai status kepercayaan dari node saat ini diperoleh berdasarkan nilai reputasi node tersebut. Dengan pendekatan ini, diharapkan dapat meningkatkan integritas dan efisiensi model konsensus DPoS serta mendorong partisipasi lebih aktif dari seluruh pemegang mata uang [15].

E. *Proof of Authority* (PoA)

Dalam model konsensu *Proof of Authority* (PoA), para validator (otoritas) mempertaruhkan reputasi dan identitas mereka dalam jaringan alih-alih mempertaruhkan token atau koin asli. Mekanisme konsensus PoA dapat bervariasi tergantung pada implementasinya, namun secara umum terdapat beberapa syarat seperti, validator harus mengonfirmasi identitas asli mereka, dan wajib mempertaruhkan reputasinya. Dalam kondisi tertentu, juga menginvestasikan sejumlah dana. Kandidat yang menjalani proses validasi yang lebih ketat akan tertarik untuk berkomitmen jangka panjang terhadap *blockchain* keputusan.

Keuntungan utama dari penggunaan mekanisme konsensus PoA meliputi toleransi risiko yang tinggi, kecuali dalam kasus di mana 51% validator bertindak dengan niat jahat, serta waktu pembuatan blok yang dapat diprediksi. PoA juga memiliki tingkat transaksi yang tinggi dan tidak memerlukan pemborosan sumber daya untuk pemrosesan. Namun, terdapat beberapa keterbatasan dalam model PoA seperti, identitas agen penentu (DA) yang diketahui oleh publik, sehingga pihak ketiga dapat mencoba untuk memanipulasi mereka. Serta mekanisme PoA tidak sepenuhnya terdesentralisasi karena bergantung pada individu-individu yang dipercaya yang beroperasi di jaringan *Decision Blockchain* [16] .

3.2 Kelebihan dan Kekurangan System *Blockchain*

Adapun kelebihan dan kekurangan yang dimiliki dalam *blockchain* adalah sebagai berikut:

A. Kelebihan dari system *blockchain*

Blockchain memiliki sejumlah keuntungan yang menjadikannya teknologi yang menarik dalam berbagai aplikasi. Seperti, tingkat keamanan tinggi, transparan, efisien, dapat diakses siapa saja, bisa digunakan di berbagai industri dan *history* transaksi yang permanen.

B. Kekurangan dari sistem *blockchain* [2] [3]

Blockchain juga memiliki sejumlah kekurangan seperti, keterbatasan skalabilitas, biaya transaksi yang dapat meningkat secara signifikan, konsumsi energi yang tinggi, adanya tantangan terhadap regulasi, dan terjadinya kegagalan teknologi atau serangan.

3.3 Cara Kerja Blockchain

Sistem *blockchain* dimulai ketika sebuah blok menyimpan sebuah data baru. Sistem ini terdiri dari dua jenis *record*, yaitu transaksi dan blok. Setiap blok akan terisi oleh *hash* kriptografi yang kemudian akan membentuk jaringan. *Hash* kriptografi berfungsi untuk mengambil data-data dari blok asal, lalu diubah menjadi *compact string*. *String* ini digunakan sebagai alarm pendeteksi apabila ditemukan adanya potensi *sabotase* atau penyimpangan data lainnya. *Blockchain* ini bekerja dengan sistem yang terdesentralisasi, di mana teknologi ini tidak terikat pada satu otoritas apapun secara penuh, melainkan terpecah-pecah ke setiap komputer yang sudah diinstalkan *software* [4].

Di dalam sistem *blockchain*, setiap catatan yang disebut *block* akan dihubungkan satu sama lain dalam satu daftar panjang yang dikenal dengan *chain*. Setiap blok harus memiliki *hash* kriptografinya sendiri serta *hash* dari blok sebelumnya agar tetap terhubung. *Hash* berisi nomor alfanumerik unik yang dihitung berdasarkan data dari blok itu sendiri, *timestamp*, serta *hash* dari blok sebelumnya. Basis data *blockchain* menyimpan data dalam struktur yang dikelompokkan. Blok yang sudah dimasukkan ke dalam *chain* berfungsi sebagai catatan data permanen, disimpan dengan *timestamp* yang jelas, dan terhubung ke dalam jaringan tanpa batas [17].

3.4 Cara Kerja Bitcoin

Bitcoin memanfaatkan teknik tanda tangan elektronik ECDSA (Elliptic Curve Digital Sig- nature Algorithm) dengan spesifikasi secp256k1, untuk memastikan apakah pengguna merupakan pemilik sah atas uang yang berada dalam alamat *bitcoin* yang diklaim. Fungsi *hash* merupakan salah satu teknik kriptografi untuk menghitung nilai unik dari sebuah data. Fungsi *hash* dapat diibaratkan sebagai sidik jari elektronik dari informasi elektronik. Yang berguna untuk menentukan orisinalitas sebuah dokumen elektronik. *Bitcoin* menggunakan beberapa fungsi hash seperti, RIPEMD160 dan SHA256. RIPEMD160 digunakan dalam proses penghitungan alamat *bitcoin*, sementara SHA256 digunakan dalam penghitungan nilai *hash* transaksi *bitcoin*.

Transaksi ini mendefinisikan satu koin elektronik sebagai satu rangkaian tandatangan digital. Setiap pemilik dari koin mentransfer ke pemilik selanjutnya dengan membubuhkan tandatangan digital pada *hash* dari transaksi sebelumnya dan *public key* dari pemilik selanjutnya pada akhiran koin. Penerima pembayaran (*payee*) dapat memverifikasi

tandatangan untuk memastikan rantai kepemilikan. Untuk mengimplementasikan *timestamp server* yang terdistribusi secara *peer-to-peer*, kita perlu menggunakan sistem *proof-of-work* yang mirip dengan *Adam Back's Hashcash* [6], daripada *newspaper* atau pos pada *Usenet*. *Proof-of-work* melibatkan proses pemindaian dari nilai yang jika melalui proses *hashing*, Jumlah rata-rata usaha yang diperlukan berbanding eksponensial dengan jumlah bit nol yang diperlukan dan bisa diverifikasi dengan mengeksekusi sebuah *hash*. Untuk jaringan timestamp ini, *proof-of-work* diimplemetasikan dengan deret inkremental dari kejadian (*nonce*) dalam blok sampai didapat suatu nilai yang dapat memberikan *hash* dari suatu blok banyaknya bit nol yang dibutuhkan. Begitu tenaga komputasi ditingkatkan untuk memenuhi kebutuhan *proof-of-work*, blok tersebut tidak dapat diubah tanpa mengulang proses. Untuk mengubah blok tersebut mengharuskan untuk mengulang pembuatan blok-blok setelahnya juga. *Proof-of-work* juga mengatasi masalah dalam menentukan pembuat keputusan mayoritas. Jika keputusan mayoritas dibuat berdasarkan kepada satu IP *address* untuk satu suara, dapat ditumbangkan oleh siapapun yang dapat mengalokasikan banyak IP. *Proof-of-work* pada dasarnya adalah satu CPU satu suara (*one-CPU-one-vote*). Keputusan mayoritas ditentukan oleh rantai terpanjang, yang mempunyai usaha *proof-of-work* terbanyak. Jika mayoritas kekuatan CPU dikendalikan oleh titik-titik komputasi yang jujur, rantai yang jujur dapat tumbuh lebih cepat dan mengalahkan rantai lainnya. Untuk mengubah blok yang sudah ada, penyerang perlu membuat ulang *proof-of-work* blok tersebut dan semua blok sesudahnya dan kemudian mengejar dan menyusul kerja titik-titik komputasi yang jujur. Kami akan perlihatkan nanti kemungkinan penyerang yang lebih lambat yang berusaha untuk mengejar menghilang secara eksponensial ketika blok-blok berikutnya ditambahkan. Untuk mengkompensasi peningkatan kecepatan perangkat keras dan minat menjalankan titik komputasi yang berubah-ubah seiring perkembangan waktu, tingkat kesulitan dari *proof-of-work* ditentukan oleh target rata-rata jumlah blok per jam yang selalu berubah-ubah juga[2].

3.5 Cara Kerja Ethereum

Ethereum beroperasi pada jaringan komputer terdesentralisasi, dengan *Ether* (ETH) sebagai mata uangnya. *Ethereum* diumumkan pada tahun 2014 dan diluncurkan pada tahun 2015 dan *platform* ini mengintegrasikan bahasa pemrograman yang lengkap secara *Turing*, sehingga memungkinkan untuk mengekspresikan semua perhitungan praktis dalam bentuk *smart contracts*. *Smart contracts* adalah program komputer yang memungkinkan pengguna untuk membuat aturan mereka sendiri terkait kepemilikan. Pengguna dapat melakukan transaksi *Ether* melalui s*mart contracts*. Pengguna *Ether* menggunakan pasangan kunci privat dan publik yang disediakan oleh Algoritma Tanda Tangan Digital Kurva Eliptik (ECDSA) untuk memastikan keamanan transaksi.

Proses kerja *Ethereum* dimulai ketika seorang pengembang menciptakan aplikasi terdesentralisasi (DApp) di atas *blockchain Ethereum*. DApp ini dapat diakses oleh klien untuk melakukan transaksi. Transaksi tersebut kemudian dikirim ke jaringan untuk diproses. *Miners* dalam jaringan *Ethereum* akan memverifikasi transaksi bahwa semua data valid dan sesuai dengan aturan yang telah ditetapkan. Setelah verifikasi, transaksi-transaksi tersebut akan dikelompokkan untuk ditambahkan ke dalam blok baru. Proses ini melibatkan *Miners* yang bersaing untuk menyelesaikan tantangan kriptografi untuk membuat blok baru. Setelah blok baru terbentuk, semua node dalam jaringan akan memeriksa keabsahan blok tersebut

untuk memastikan tidak ada kesalahan atau penipuan. Jika semua node setuju bahwa blok tersebut valid, blok baru akan ditambahkan ke dalam *blockchain*. Sebagai imbalan, m*iners* akan menerima sejumlah *Ether*. Proses ini berulang secara terus-menerus setiap kali transaksi baru dilakukan [18].

3.6 Aplikasi Terdesentralisasi – DApps

Aplikasi Terdesentralisasi (*DApp*) adalah aplikasi yang dibangun di atas jaringan *blockchain*, menggunakan *smart contract* dan halaman *web*site. *DApp* dapat memanfaatkan *smart contract* yang telah dibuat orang lain, mirip dengan *API* terbuka. *DApp* bekerja tanpa server karena semua operasinya adalah *read and write* dari *blockchain*. *DApp* memiliki *frontend* untuk me-*render* halaman dan menggunakan dompet untuk berinteraksi dengan *blockchain*. Dompet ini mengelola kunci kriptografi dan alamat *blockchain* untuk identifikasi dan otentikasi pengguna. *DApp* tidak dikontrol oleh organisasi terpusat, sehingga mengurangi kerentanan terhadap serangan dan korupsi. Meski konsep aplikasi terdesentralisasi sudah ada sebelum *blockchain* (misalnya *BitTorrent*), istilah *DApp* kini lebih merujuk pada aplikasi berbasis *blockchain* yang menawarkan sistem yang lebih aman dan transparan [19][20]. Beberapa kategori, seperti *Finance* dan *Exchanges*, menjadi populer karena keterkaitannya dengan *cryptocurrency* dan *Ethereum*. Kategori *Games* mencakup 29,5% dari total *DApps*, tetapi hanya 8,4% pengguna. Di sisi lain, kategori *Exchanges* dan *Finance* memiliki banyak pengguna (35,4% dan 23,5%) serta volume transaksi yang signifikan (61,5% dan 25,6%). Kategori lain seperti *Identity*, *Media*, *Social*, dan *Health* masih memiliki sedikit pengguna dan transaksi, menandakan potensi tetapi memerlukan lebih banyak verifikasi dalam penggunaan praktis. Kategori *High-risk* ditandai untuk *DApps* berisiko tinggi, seperti skema Ponzi [21].

Aplikasi terdesentralisasi diklasifikasikan menjadi dua kelas; *fully anonymous decentralized applications* dan *reputation-based decentralized applications*. Namun, terdapat area abu-abu yang cukup besar di antara kedua jenis ini. Oleh karena itu, definisi aplikasi terdesentralisasi berbasis *blockchain* masih belum terdefinisi [19]. Berbagai arsitektur *DApps* dibagi ke dalam beberapa sub-bagian [19]:

1. *Native Client* sebagai *DApp*: Pengguna menjalankan klien pada jaringan *peer-to-peer* untuk mentransfer *Bitcoin*. Arsitektur ini digunakan oleh banyak *cryptocurrency* awal seperti *Litecoin* dan *PPcoin*
2. *Smart Contract* sebagai *DApp*: Pengembang dapat menulis *smart contract* di *blockchain* seperti *Ethereum* untuk mencatat informasi yang diinginkan.
3. *Web & Contract* sebagai *DApp*: Pengembang *DApp* membuat antarmuka web untuk *smart contract* agar pengguna dapat mengakses *DApp* melalui *browser* web yang terhubung ke *blockchain*.
4. *Fully-Decentralized DApp*: *Ethereum* digunakan untuk logika terdesentralisasi, *Swarm* untuk penyimpanan terdesentralisasi, dan *Whisper* untuk pesan terdesentralisasi. Penyimpanan antarmuka depan tidak bergantung pada layanan terpusat tetapi pada sistem file terdesentralisasi seperti *IPFS*.

Tiga bidang masalah yang dihadapi oleh aplikasi terdesentralisasi (*DApps*), ekonomi, keamanan, dan kinerja[19]:

1. Ekonomi: bagaimana menarik pengguna melalui insentif ekonomi seperti token atau biaya transaksi dan risiko penipuan dan volatilitas pasar,

2. Keamanan: rentan terhadap serangan pada lapisan web, *smart contract*, dan *blockchain*.
3. Kinerja Rendah: Kinerja *DApps* masih belum memadai untuk aplikasi harian, terutama karena *throughput blockchain* yang rendah..

3.7 Teknologi Blockchain: Masalah Keamanan dan Privasi

Blockchain dapat difungsikan sebagai *private*/*public blockchain*. B*lockchain* juga memiliki kemampuan menerima data, memvalidasi, dan memberikan kepercayaan serta menyediakan data bagi yang membutuhkannya. Terdapat tiga jenis dasar dari *blockchain*, yaitu [22]:

1. *Blockchain* yang diizinkan merupakan *blockchain* yang tidak dapat mengeluarkan transaksi yang mereka lakukan sendiri ataupun melihat catatannya serta bergabung dengan suatu komunitas secara bebas, merupakan tindakan *blockchain* yang diizinkan
2. *Blockchain* yang tidak diizinkan merupakan *blockchain* yang sifatnya tidak umum atau terbuka untuk semua orang yang ingin mengaksesnya.
3. *Hybrid blockchain* merupakan gabungan dari *blockchain* publik dan *blockchain* pribadi. Pada jaringan ini data data *blockchain* yang tidak diizinkan tetap dapat diakses dari tempat *blockchain* dengan menggunakan hak akses tertentu yang disimpan. Jenis *blockchain* ini tidak terbuka untuk semua orang, namun Blockchain ini menyediakan fitur dasar secara diam-diam seperti keterlancaran, integrasi dan keamanan.

Blockchain berpotensi besar untuk membawa dampak positif pada berbagai sektor, namun juga menimbulkan tantangan keamanan dan privasi yang signifikan. Beberapa solusi yang dapat diterapkan antara lain [22]:

1. Keamanan data: Menggunakan teknologi enkripsi untuk melindungi data saat disimpan dan ditransmisikan.
2. Privasi pengguna: memberikan pengguna kontrol atas data pribadi mereka dan memberikan transparansi dalam pengumpulan dan penggunaan data.
3. Keamanan sistem: menggunakan teknologi keamanan seperti otentikasi dan enkripsi data, *firewall*, dan pemantauan jaringan secara terus menerus.

Blockchain memiliki tantangan besar dalam hal keamanan dan privasi data seperti integritas data, otentikasi, otorisasi, skalabilitas, dan efisiensi. Teknologi kriptografi dapat digunakan untuk memastikan keamanan data, penggunaan mekanisme otentikasi dan otorisasi yang kuat, serta penggunaan teknologi machine learning untuk mendeteksi serangan keamanan secara cepat dan akurat [22].

3.8 Teknologi Blockchain di Bidang Energi: Peluang dan Tantangan

Teknologi blockchain memberikan potensi yang signifikan dalam industri energi, terutama dalam meningkatkan efisiensi, transparansi, dan desentralisasi melalui sistem perdagangan energi *peer-to-peer* (P2P). Dengan memanfaatkan blockchain, individu dan komunitas dapat melakukan transaksi energi terbarukan, seperti energi matahari atau angin, secara langsung tanpa perlu adanya perantara. Teknologi ini memungkinkan interaksi langsung antara konsumen dan produsen energi, atau yang dikenal sebagai prosumer, sehingga menciptakan pasar energi yang lebih terdistribusi dan efisien. Hal ini meningkatkan transparansi dalam transaksi energi dan juga memungkinkan pengelolaan sumber daya yang

lebih baik dan aman [23]. Salah satu contoh nyata dari penerapan teknologi ini adalah proyek microgrid berbasis blockchain di *Brooklyn*, *New York*, di mana warga dapat melakukan perdagangan energi surya secara lokal [24].

B*lockchain* juga berkontribusi dalam memperkuat ketahanan sistem jaringan listrik. Sistem ini mencatat transaksi secara otomatis melalui pengukur pintar, yang tidak hanya mengoptimalkan distribusi energi, tetapi juga menjaga keamanan data dalam jaringan yang semakin terdesentralisasi [25]. Contohnya, beberapa perusahaan energi telah mulai mengadopsi *platform* berbasis *blockchain* untuk mengotomatisasi perdagangan energi antar individu, seperti pemilik panel surya yang dapat menjual kelebihan energi mereka kepada tetangga [26].

Teknologi blockchain mulai diterapkan untuk mengelola distribusi energi serta mencatat produksi dari sumber-sumber energi terbarukan [27]. Teknologi ini memiliki potensi yang signifikan dalam mengurangi emisi karbon, meningkatkan kemandirian energi, dan mendorong efisiensi dalam pemanfaatan energi terbarukan [23]. Tetapi, penerapan blockchain dalam sektor energi masih menghadapi berbagai tantangan yang signifikan seperti, kurangnya infrastruktur kelembagaan dan regulasi yang mendukung perkembangan teknologi ini [25].

Untuk mengoptimalkan potensi teknologi blockchain dalam sektor energi, diperlukan kerjasama antar sektor yang melibatkan berbagai pihak. Dan penting juga untuk mengembangkan kebijakan dan regulasi yang lebih adaptif dan fleksibel terhadap perubahan teknologi, yang akan menjadi faktor penting dalam mendorong adopsi yang lebih luas. Dalam konteks yang lebih luas, blockchain tidak hanya mendukung transisi menuju energi terbarukan dengan cara yang lebih efisien, tetapi juga menciptakan model distribusi energi yang lebih kuat dan berkelanjutan, serta membuka peluang untuk inovasi bisnis baru di masa depan [23],[26],[24].

4. KESIMPULAN

Teknologi blockchain telah mengalami perkembangan yang signifikan sejak pertama kali diperkenalkan dalam konteks Bitcoin oleh Satoshi Nakamoto pada tahun 2008. Seiring berjalannya waktu, teknologi ini tidak hanya terbatas pada cryptocurrency, tetapi juga telah diadopsi di berbagai sektor, termasuk keuangan, logistik, kesehatan, pemasaran, dan energi. Dengan karakteristik utama seperti desentralisasi, transparansi, dan keamanan, blockchain menawarkan solusi inovatif untuk pengelolaan data dan transaksi yang lebih efisien.

Berbagai mekanisme konsensus, seperti Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), dan Delegated Proof of Stake (DPoS), masing-masing memiliki kelebihan dan kekurangan dalam menjaga integritas serta keamanan data di jaringan blockchain. PoW dikenal karena tingkat keamanannya yang tinggi, meskipun memerlukan konsumsi energi yang besar, sedangkan PoS menawarkan efisiensi energi yang lebih baik. Di sisi lain, PBFT dan DPoS lebih mengutamakan kecepatan dan efisiensi skalabilitas, menjadikannya pilihan menarik untuk berbagai aplikasi.

Dalam praktiknya, blockchain dapat meningkatkan kepercayaan melalui catatan transaksi yang transparan dan tidak dapat diubah. Hal ini menciptakan lingkungan yang aman dan dapat diandalkan bagi pelaku bisnis dan pengguna. Namun, tantangan seperti ketergantungan pada teknologi, risiko keamanan seperti serangan 51%, dan isu skalabilitas masih menjadi hambatan yang perlu diatasi.

Secara keseluruhan, teknologi blockchain memiliki potensi besar untuk mendukung transformasi digital di berbagai industri. Penerapan yang tepat dengan mitigasi risiko yang terencana akan memungkinkan blockchain menjadi fondasi utama bagi sistem yang lebih aman, efisien, dan transparan di masa depan. Oleh karena itu, kolaborasi antara pemerintah, sektor industri, dan komunitas teknologi sangat penting untuk mengembangkan regulasi yang adaptif dan menciptakan lingkungan yang kondusif bagi inovasi blockchain

REFERENSI

[1] K. Teknologi, "Mengenal Blockchain dan pengaruhnya dalam bisnis digital," Himpunan Mahasiswa Informatika ITERA.
[2] M. Bahanan and M. Wahyudi, "Analisis Pengaruh Penggunaan Teknologi Blockchain Dalam Transaksi Keuangan Pada Perbankan Syariah," *Jurnal Ekonomi Syariah*, vol. 2, no. 1, Apr. 2023.
[3] Z. Munawar, N. Indah Putri, I. Iswanto, and D. Widhiantoro, "Analisis Keamanan Pada Teknologi Blockchain," *Infotronik : Jurnal Teknologi Informasi dan Elektronika*, vol. 8, no. 2, p. 67, Dec. 2023, doi: 10.32897/infotronik.2023.8.2.2062.
[4] T. Redaksi, "Mengenal Apa Itu Blockchain, Teknologi yang Mengubah Dunia," CNBC Indonesia.
[5] T. W. E. Suryawijaya, "Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia Strengthening Data Security through Blockchain Technology: Exploring Successful Implementations in Digital Transformation in Indonesia," *Jurnal Studi Kebijakan Publik*, vol. 2, no. 1, pp. 55–67, May 2023, doi: 10.21787/jskp.2.2023.55-67.
[6] Siswanto, "Systematic Review Sebagai Metode Penelitian Untuk Mensintesis Hasil-Hasil Penelitian (Sebuah Pengantar)," *Buletin Penelitian Sistem Kesehatan*, vol. 13, no. 4, pp. 326–333, Oct. 2010.
[7] H. Chakka, "Who is Real Bitcoin's Creator Satoshi Nakamoto?," https://www.analyticsinsight.net/bitcoin/who-is-real-bitcoins-creator-satoshi-nakamoto.
[8] A. Harnoy, "Blockchain: Decentralized Ledgers Enabling Peer to Peer Payments without a Trusted Intermediary - SGR Law." Accessed: Nov. 05, 2024. [Online]. Available: https://www.sgrlaw.com/blockchain-decentralized-ledgers/
[9] Y. Hayes, Adam; Rasure, Erika; Perez, "Who Is Satoshi Nakamoto?" Accessed: Nov. 05, 2024. [Online]. Available: https://www.investopedia.com/terms/s/satoshi-nakamoto.asp
[10] Harshini. Chakka, "Who is Real Bitcoin's Creator Satoshi Nakamoto?" Accessed: Nov. 05, 2024. [Online]. Available: https://www.analyticsinsight.net/bitcoin/who-is-real-bitcoins-creator-satoshi-nakamoto
[11] Vida, "Contoh Blockchain dan Penerapannya di Berbagai Industri," Vida.id.
[12] V. Palidita Febriana, T. Suci Wulandari, Z. Azmi, and U. Muhammadiyah Riau, "Penggunaan Teknologi Blockchain Dalam Sistem Informasi Akuntansi : Peluang Dan Tantangan," 2024.
[13] B. Sriman, S. Ganesh Kumar, and P. Shamili, "Blockchain Technology: Consensus Protocol Proof of Work and Proof of Stake," in *Advances in Intelligent Systems and Computing*, Springer Science and Business Media Deutschland GmbH, 2021, pp. 395–406. doi: 10.1007/978-981-15-5566-4_34.
[14] X. Zheng and W. Feng, "Research on Practical Byzantine Fault Tolerant Consensus Algorithm Based on Blockchain," in *IOP Conference Series: Earth and Environmental Science*, IOP Publishing Ltd, Mar. 2021. doi: 10.1088/1742-6596/1802/3/032022.

[15] Q. Hu, B. Yan, Y. Han, and J. Yu, "An Improved Delegated Proof of Stake Consensus Algorithm," in *Procedia Computer Science*, Elsevier B.V., 2021, pp. 341–346. doi: 10.1016/j.procs.2021.04.109.
[16] M. A. Manolache, S. Manolache, and N. Tapus, "Decision Making using the Blockchain Proof of Authority Consensus," in *Procedia Computer Science*, Elsevier B.V., 2021, pp. 580–588. doi: 10.1016/j.procs.2022.01.071.
[17] T. P. Utomo, "Implementasi Teknologi Blockchain Di," *Buletin Perpustakaan Universitas Islam Indonesia*, vol. 4, no. 2, pp. 173–200, 2021.
[18] H. Li, "The Applications of Cryptocurrency: Evidence from Ethereum," 2022.
[19] S. Tikhomirov, "Ethereum: state of knowledge and research perspectives."
[20] P. Zheng, Z. Jiang, J. Wu, and Z. Zheng, "Blockchain-Based Decentralized Application: A Survey," *IEEE Open Journal of the Computer Society*, vol. 4, pp. 121–133, Mar. 2023, doi: 10.1109/OJCS.2023.3251854.
[21] A. Mattew and M. A. Suwarno, "Rancang Bangun Aplikasi Donasi Terdesentralisasi Berbasis Blockchain," *Jurnal Ikraith-Informatika*, vol. 7, no. 2, pp. 23–32, Jul. 2023.
[22] K. Wu, Y. Ma, G. Huang, and X. Liu, "A First Look at Blockchain-based Decentralized Applications," Sep. 2019.
[23] A. J. Indrawan, "IoT dan Blockchain: Tinjauan Tantangan Solusi Keamanan dan Privasi," Apr. 2023, doi: 10.13140/RG.2.2.23977.40806.
[24] Mulyati, Padeli, Chakim Mochamad Heru Riza, N. Azizah, and D. Julianingsih, "Implikasi Pengembangan Energi Terdistribusi di Lingkungan Institusi Berbasis Blockchain," *Seminar Nasional Corisindo*, pp. 38–46, Aug. 2022.
[25] S. Ariawan, "Green digitalisasi sebagai perwujudan mandat budaya: Perspektif etika Kristen dalam pelestarian lingkungan," *Jurnal Teologi dan Pendidikan Agama Kristen*, vol. 10, no. 1, pp. 275–287, Apr. 2024.
[26] A. A. R. Nasution and M. S. Hasibuan, "Analisis Keamanan Jaringan Smart Grid PLN Menggunakan Metode Blockchain dalam Konteks Kemananan Cyber," *Journal Of Computer Science And Informatics Engineering (CoSIE)*, vol. 3, no. 2, pp. 64–73, Apr. 2024.
[27] W. Paul, "Pengembangan Uang Rupiah Digital Melalui Teknologi Blockchain," *Jurnal Al-Amar (JAA)*, vol. 3, no. 1, pp. 17–31, Jan. 2022.
[28] C. J. Indranata, "Analisis Manajemen Zakat Berbasis Blockchain Technology Sebagai Strategi Optimaliasasi Kebijakan Suistainable Development Goals," Yogyakarta, Feb. 2024.