

Kajian Perkembangan Teknologi Blockchain dan Implementasinya pada Berbagai Sektor di Era Industri 4.0

Aswadul Fitri Saiful Rahman^{1*}, Andani Achmad²

¹Teknik Elektro, Fakultas Teknologi Industri, Universitas Balikpapan

²Departemen Teknik Elektro, Fakultas Teknik, Universitas Hasanuddin

¹aswadul864@uniba-bpn.ac.id, ²andani@unhas.ac.id

*Penulis Korespondensi

Abstract— *Blockchain is a rapidly evolving distributed technology that plays an important role in supporting digital transformation in the Industry 4.0 era. This technology is capable of improving data security, transparency, integrity, and privacy through decentralization mechanisms and consensus algorithms implemented across various blockchain platforms. The development of blockchain is no longer limited to cryptocurrency applications, but has also expanded to smart contracts and decentralized applications (DApps) that support a wide range of digital services in various industrial sectors. This paper aims to examine the development of blockchain technology, including blockchain evolution and architecture, blockchain access types, consensus mechanisms, and its implementation across multiple sectors. The research method used in this study is a literature review by analyzing various scientific references related to blockchain development and applications. The results show that each type of blockchain, namely public, private, and consortium, has different characteristics and implementations depending on organizational and industrial requirements. In addition, the development of consensus algorithms continues to improve system efficiency, scalability, and security. Blockchain has been widely implemented in various sectors, such as finance, healthcare, education, logistics, government, and the Internet of Things (IoT). However, blockchain implementation still faces several challenges, including energy consumption, network scalability, interoperability between platforms, as well as regulatory, security, and data privacy issues. This study is expected to serve as a reference for the development and implementation of more adaptive, secure, and efficient blockchain technology in the Industry 4.0 era.*

Intisari— *Blockchain merupakan teknologi terdistribusi yang berkembang pesat dan memiliki peran penting dalam mendukung transformasi digital pada era Industri 4.0. Teknologi ini mampu meningkatkan keamanan, transparansi, integritas, dan privasi data melalui mekanisme desentralisasi serta algoritma konsensus yang diterapkan pada berbagai platform Blockchain. Perkembangan Blockchain tidak hanya terbatas pada *cryptocurrency*, tetapi juga telah berkembang ke *smart contract* dan *decentralized applications (DApps)* yang mendukung berbagai layanan digital di berbagai sektor industri. Makalah ini bertujuan untuk mengkaji perkembangan teknologi Blockchain, meliputi evolusi dan arsitektur Blockchain, tipe akses data Blockchain, mekanisme konsensus, serta implementasinya pada berbagai sektor. Metode yang digunakan dalam penelitian ini adalah studi literatur dengan menganalisis berbagai referensi ilmiah terkait perkembangan dan penerapan Blockchain. Hasil kajian menunjukkan bahwa setiap jenis Blockchain, baik *public*, *private*, maupun *consortium*, memiliki karakteristik dan penerapan yang berbeda sesuai kebutuhan organisasi dan industri. Selain itu, perkembangan algoritma konsensus terus dilakukan untuk meningkatkan efisiensi, skalabilitas, dan keamanan sistem Blockchain. Implementasi Blockchain telah diterapkan pada berbagai bidang, seperti keuangan, kesehatan, pendidikan, logistik, pemerintahan, dan *Internet of Things (IoT)*. Namun demikian, implementasi Blockchain masih menghadapi beberapa tantangan,*

seperti konsumsi energi, skalabilitas jaringan, interoperabilitas antarplatform, serta regulasi dan privasi data. Kajian ini diharapkan dapat menjadi referensi dalam pengembangan dan implementasi teknologi Blockchain yang lebih adaptif, aman, dan efisien pada era Industri 4.0.

Kata Kunci— *Blockchain, Terdistribusi, Smart Contract, Konsensus, Decentralization Applications.*

I. PENDAHULUAN

Revolusi industri 4.0 yang berkembang saat ini merupakan teknologi disrupti, teknologi yang dipengaruhi oleh perkembangan sistem digital atau perkembangan dengan sistem lama akan ditransformasikan ke sistem masa depan atau sistem digital dalam bidang industri. Industri 4.0 sangat erat kaitannya dengan sistem cerdas dan otomatisasi industri, hal ini didukung dengan pengambilan keputusan secara otomatis melalui komputer yang saling terhubung dan berkomunikasi. Teknologi ini merupakan kombinasi dari infrastruktur jaringan komputer dan Internet of things. Tantangan penggunaan jaringan internet salah satunya yaitu keamanan data dan jaringan. Salah satu teknologi disrupti yaitu blockchain. *Blockchain* adalah struktur data terdistribusi yang direplikasi dan dibagikan di antara anggota jaringan. Teknologi ini sudah dipelajari mulai tahun 2008 dan diterapkan pada bitcoin [1], ini merupakan solusi dari permasalahan tentang kepercayaan pada transaksi [2]. Transaksi bitcoin ini yang menjadi dasar terciptanya algoritma blockchain yang pertama dan dikenal sebagai *proof-of-work* [1].

Blockchain merupakan teknologi yang dapat digunakan untuk meningkatkan keamanan, privasi dan transparansi data pada perusahaan kecil atau besar. Beberapa bidang yang menggunakan blockchain mendapatkan keuntungan prospektif, contohnya blockchain dapat memberikan kepercayaan pada transaksi keuangan digital [3]. Teknologi ini menyediakan infrastruktur teknis berbagai tingkat platform dan penerapan *decentralization applications (DApp)* yang mendukung aplikasi industri dengan layanan luas dengan domain yang berbeda [4], seperti *Ethereum* [5] dengan *Ethereum Blockchain*, *Hyperledger* dengan *Hyperledger Fabric* [6].

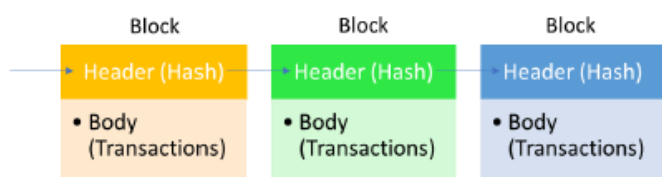
II. EVOLUTION DAN ARSITEKTUR BLOCKCHAIN

Pada bagian ini menguraikan tentang klasifikasi teknologi Blockchain.

A. Blockchain 1.0 (Cryptocurrencies)

Pada tahap blockchain 1.0, teknologi yang utama yang dikembangkan adalah mata uang kripto (cryptocurrency) atau yang terkenal yaitu bitcoin, selain itu ada Litecoin [7], Dogecoin dan yang berkembang saat ini sekitar 700 jenis cryptocurency [8]. Lapisan teknologi cryptocurrency dibagi menjadi 2 lapisan, lapisan buku besar terdesentralisasi dan lapisan protokol. Di dalam sistem bitcoin proses penambangan dan validasi memakan waktu sekita 7-8 menit [9]. Setiap transaksi disimpan dalam daftar dan kalau sudah mencapai ukuran tertentu, daftar baru akan dibuat dan daftar yang alam akan dihash, kode hash daftar lama akan menjadi nilai awal dari daftar baru sehingga setiap blok akan dirantai dan divalidasi satu dengan yang lain [10]. Sekelompok pengguna akan bergabung bersama dalam jaringan P2P untuk mengelola verifikasi catatan buku besar (ledger).

Struktur blockchain terdiri dari dua bagian yaitu Block Header dan Block Body, seperti pada gambar 1. Block Header meliputi Block version, Merkle Tree Root Hash, Time Stamp, nBits, Nonce dan Parent Block Hash, sedangkan Block Body meliputi transaksi dan penghitung transaksi. Kapasitas maksimum blok untuk menyimpan transaksi ditentukan oleh ukuran blok dan ukuran setiap transaksi yang ada di dalamnya [11]. Transaksi bitcoin dan Distibuted ledger lainnya berukuran sekitar beberapa ratus byte, bahkan dengan penggunaan data yang sedikit, node yang kurang beruntung secara bertahap akan meninggalkan permainan penambangan pada sebagian besar sistem distributed ledger [12]. Algoritma konsensus pertama yang digunakan Blockchain 1.0 adalah Proof-of-Work (PoW). Gambar 1 merupakan block arsitektur Blockchain.



Gambar 1. Block di dalam Arsitektur Blockchain [11]

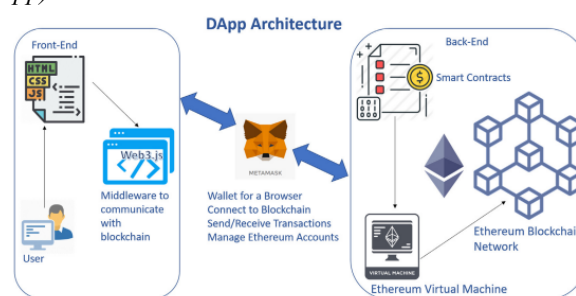
B. Blockchain 2.0 (Smart Contract)

Smart Contract atau kontrak pintar sebenarnya konsep ini sudah ada sejak tahun 1994 yang didefinisikan sebagai komputerisasi protokol transaksi yang melaksanakan ketentuan sebuah kontrak. Tujuan dari komputerisasi ini untuk menterjemahkan klausak kontrak ke dalam kode dan diimplementasikan ke dalam perangkat lunak atau keras yang akan bekerja secara otomatis dengan meminimalkan

kebutuhan perantara yang terpercaya. Smart contract bersifat deterministik, masukan yang sama akan menghasilkan keluaran yang sama [13]. Smart contract merupakan sebuah program komputer di dalam perangkat lunak blockchain seperti *Ethereum* [14], *Hyperledger Fabric*, *NEM*, *STELLAR*, *Waves*, dan *Corda* [15], jadi secara otomatis akan melakukan perjanjian antara dua pihak atau lebih tanpa perantara yang terpercaya. Riwayat transaksi disimpan di blockchain yang mirip dengan mata uang digital, status kontrak dan aset anggota ditentukan oleh urutan transaksi di blockchain [16].

Ethereum merupakan khas dari blockchain 2.0, setiap node mempunyai EVM (Ethereum Virtual Machine) atau bahasa pemrograman yang menjalankan smart contract, begitu juga dengan sistem blockchain yang lain seperti RSK:Solidity, Stellar:Transaction chains, Monax:EVM bytecode, dan Lisk:JavaScript [17] [8]. *Smart Contract* disebut juga *Decentralized Application (DApps)* yang ringan. *DApp* ini sama dengan *traditional centralized application*, memiliki klien, server dan teknologi *middleware*, tetapi data dan operasi utama disimpan dalam smart contract di jaringan blockchain Ethereum. Komunikasi diantara smart contract di *DApps* dicapai menggunakan transaksi yang disebut sebagai permintaan kontrak (request contract).

DApp mempunyai karakteristik umum sebagai berikut [18]: 1) *Decentralized*, setiap transaksi dan operasi dalam *DApp* harus ditangkap di jaringan publik dan terdesentralisasi untuk mengatasi keterbatasan *traditional centralized application*. 2) *Incentivized*, *Penambang / mitra* pada jaringan *Blockchain* seharusnya diberikan insentif yang sesuai dengan token kriptografi untuk inialisasi dan menyelesaikan transaksi. 3) *Protocol*, *DApp* dibangun berdasarkan protokol konsensus, jadi semua peserta harus menyetujui algoritma kriptografi sebagai bukti nilai (*proof of value*). 4) *Public (open source)*, *DApp* harus tersedia untuk publik untuk dianalisis. Gambar 2. Menunjukkan arsitektur *Decentralized Application (DApp)*.



Gambar 2. Arsitektur Decentralized Application (DApp) [18].

Eksekusi *Smart Contract* yang benar tidak bergantung pada pihak ketiga seperti *cryptocurrency*, protokol konsensus dibuat untuk mengatasi potensi konflik antara pihak-pihak yang terikat kontrak [19]. Platform yang menggunakan smart contract berisi fitur dasar seperti kode yang tidak bisa diubah,

buku besar yang terdesentralisasi (ledger), dan lapisan konsensus [15]. Beberapa karakteristik smart contract antara lain: *Deterministic*, *Immutable*, dan *Verifiable*, sedangkan keuntungan *smart contract* yaitu Kecepatan dan update real-time, Akurasi, Mengurangi resiko eksekusi, perantara yang lebih sedikit, biaya rendah, dan model bisnis baru [20]. Konsep desentralisasi smart contract secara umum juga mendukung transfer berbagai jenis aset seperti saham, obligasi, pinjaman, hipotek, properti pintar, dll [21]. Penerapan potensial smart contract dalam industri seperti *healthcare*, *supply chains*, *energy* dsb. Teknologi ini dapat menawarkan prosedur otomatisasi dan aksesibilitas data diberbagai sektor [22].

C. Blockchain 3.0 (Blockchain Applications)

Teknologi blockchain telah berkembang dan diterapkan dibidang industri untuk pengembangan aplikasi terdistribusi seperti pada game, Jaringan pembuatan konten, *Internet of Things*, *smart hardware*, *supply chain*, *source tracing*, *smart city*, *smart governance*, *smart mobility*, *smart environment (power, water)*, dan *smart living* [23][24]. Tahap ini dikenal sebagai blockchain 3.0 yang berfokus pada aplikasi terdistribusi dengan kinerja yang lebih baik meliputi latensi rendah, throughput tinggi, manajemen identitas yang sederhana dan transaksi yang lebih efisien dan pemeliharaan yang fleksibel untuk peningkatan sistem dan pemulihan bug yang mudah [25].

Banyak aplikasi blockchain baru yang berkembang seperti blockchain dengan cloud sebagai pusat data cloud untuk meningkatkan keamanan dan kinerja sistem, penggunaan jaringan *smart grid* untuk protokol keamanan dan otentikasi [26] [27], Teknologi ini menjanjikan pemecahan masalah terkait sistem energi masa depan karena kepercayaan terdistribusi, *anonymity*, *data integrity* dan *availability* [28]. *Blockchain* juga digunakan untuk penyimpanan data medis yang efisien dan penggunaan mekanisme berbagi [29] dengan *Blockchain* ganda, pertama untuk menyimpan data sedangkan kedua untuk berbagi data antara rumah sakit dan organisasi layanan kesehatan [30] [31], sistem informasi data medis memberikan kemampuan untuk menemukan, mempelajari, menganalisis dan bertukar informasi dengan lebih cepat dan akurat [32]. *Blockchain 3.0* merupakan platform yang berkontribusi dalam pengembangan *Smart World*, terutama untuk alokasi sumber daya dalam bentuk fisik dan asetnya [33].

III. TIPE BLOCKCHAIN

Berdasarkan penggunaan dan atribut yang berbeda, blockchain diklasifikasikan menjadi 3 jenis yaitu Public, Private dan Consortium. Jenis blockchain ini disajikan disemua versi blockchain seperti Bitcoin, Smart Contract dan aplikasi blockchain lainnya.

A. Public Blockchain

Public Blockchain memiliki buku besar (ledger) yang dapat dilihat atau diakses semua orang melalui internet dan

siapapun dapat memverifikasi dan menambahkan blok transaksi ke blockchain [34][35]. Pada sistem ini peserta tidak memerlukan ijin apapun untuk bergabung dalam jaringan [25]. Blockchain terdesentralisasi [36], untuk itu peserta dapat berpartisipasi dalam proses konsensus, membaca dan mengirim transaksi, dan memelihara buku besar (ledger) bersama-sama [37]. Blok baru dapat dipublikasikan, diakses dan divalidasi oleh semua peserta sehingga mereka mendapatkan salinan blockchain yang lengkap [38] [39].

Mekanisme konsensus yang digunakan antara lain PoW atau PoS untuk mencapai kesepakatan mengenai pembaruan sistem [40]. Setiap node memiliki sepasang kunci private/public, oleh karena itu blockchain publik tidak perlu mempercayai siapapun yang menggunakan jaringan tersebut dan setiap node dapat mengambil bagian dalam proses konsensus [41]. Bitcoin dan Ethereum adalah contoh dari public blockchain. Algoritma konsensus yang menggunakan jenis ini antara lain *Proof of Work (PoW)*, *Proof of Stake (PoS)*, *Delegated Proof of Stake (DPoS)*

B. Private Blockchain

Private blockchain hanya dapat diakses atau diijinkan untuk orang-orang tertentu dalam organisasi untuk memverifikasi dan menambahkan blok transaksi tetapi secara umum dapat dilihat semua orang melalui internet [42]. Peserta diperbolehkan bergabung dengan jaringan melalui undangan dan memainkan peran khusus untuk memelihara atau menjaga blockchain yang terdesentralisasi. Blockchain yang diijinkan dianggap lebih aman dan efisien dibandingkan dengan peserta publik. Node yang telah diotorisasi untuk membaca data juga harus diotorisasi untuk menyiarkan transaksi. Blockchain ini bersifat terpusat pada lingkungan tertutup [43], selain itu dengan sedikit peserta memiliki tingkat pemrosesan transaksi yang sangat tinggi dan waktu yang singkat dalam mendapatkan konsensus jaringan serta lebih banyak transaksi diproses dalam satu detik [44].

Jenis publik ini memiliki privasi data yang sangat kuat, jika ada data yang akan diubah harus melalui persetujuan semua node atau peserta bahwa data dapat diubah melalui konsensus [45]. Organisasi bisnis biasanya menggunakan private blockchain yang memiliki ijin untuk implementasi, misalnya Hyperledger [40]. Algoritma konsensus yang menggunakan jenis ini antara lain *Practical Byzantine Fault Tolerance (PBFT)*, *Proof of Authority (PoA)*, *Proof of Elapsed Time (PoET)*.

C. Consortium Blockchain

Blockchain ini merupakan bagian dari *Blockchain* pribadi tetapi untuk banyak organisasi dan hanya peserta yang diundang dan dipercaya yang diijinkan bergabung dan memelihara jaringan. Proses konsensus pada Consortium blockchain relatif lambat dibandingkan dengan blockchain pribadi tetapi lebih cepat dari blockchain publik [25]. Untuk

keamanan, blockchain ini menangani informasi dengan cara yang lebih terlindungi saat dilakukan perubahan dibandingkan blockchain pribadi. Perlindungan dari peretas juga lebih baik berdasarkan langkah-langkah keamanan yang diterapkan dikarenakan peserta dari berbagai organisasi. Contoh penerapan jenis ini yaitu pada Quorum, Corda, dan Sawtooth [46].

Blockchain ini dapat dilihat sebagai trade off antara desentralisasi dan privasi [47] [48], karena dikendalikan oleh beberapa organisasi yang berbeda, beberapa skema konsensus seperti PoW, PoS atau DpoS tidak lagi sesuai. Konsensus yang cocok untuk blockchain ini yaitu Byzantine Fault Tolerance dan algoritma pertama yang dibuat Practical Byzantine Fault Tolerance (PBFT) [49] yang didukung untuk output tinggi, bukti validitas yang ketat, dan sistem latensi rendah dengan kompleksitas waktu polinomial. Consortium blockchain ini populer diperusahaan besar dan pemerintahan dikarenakan biaya transaksi rendah, konsumsi energi rendah, dan tidak ada serangan 51% [50]. Algoritma konsensus yang menggunakan jenis ini antara lain *Practical Byzantine Fault Tolerance (PBFT)*, *Proof of Vote (PoV)*, *Proof of Trust (PoT)*.

IV. MEKANISME KONSENSUS

Dalam Teknologi *Blockchain* untuk memvalidasi transaksi dan mencapai konsensus terkait dampak suatu transaksi pada pembaruan buku besar (*ledger*) digunakan mekanisme konsensus. Terdapat banyak model konsensus yang diimplementasikan dengan cara yang berbeda pada setiap platform blockchain. Berikut ini klasifikasi berbagai macam algoritma konsensus yang digunakan dalam teknologi Blockchain.

A. Proof of Work (PoW)

PoW merupakan strategi konsensus yang diterapkan dalam jaringan blockchain Bitcoin. Algoritmanya memerlukan proses komputasi yang tidak mudah dalam autentikasinya. Setiap node jaringan menghitung nilai hash dari header blok yang terus bertambah. Dalam jaringan terdesentralisasi, seluruh peserta harus menghitung nilai hash secara terus menerus dengan menggunakan nonce yang berbeda sampai target tercapai [51]. *Node* yang menghitung hash disebut penambang (*miner*) dan prosedur *PoW* disebut penambang (*mining*) [41]. Fungsi hash digunakan sebagai salah satu teka-teki kriptografi dipusat algoritma konsensus PoW. Jaringan Bitcoin menggunakan fungsi hash kriptografi SHA-256 [52].

Pendekatan konsensus *PoW* untuk Bitcoin merupakan pendekatan energi yang tidak efisien, penggunaan 15.77 Terawatt hour, yaitu sekitar 0.08% dari konsumsi kebutuhan listrik dunia dan ancaman bagi iklim global karena emisi gas rumah kaca [53][54]. Daya yang sebagian besar ini dihabiskan untuk komputasi fungsi hash SHA-256 yang tidak dapat diubah. Sistem blockchain masih rentan terhadap keamanan dan serangan data integritas. Serangan ini bisa terjadi dari

konsensus *PoW* terkait manipulasi mayoritas 51% [55], konsensus mengalami penundaan karena penolakan layanan terdistribusi [56][41]. *PoW* juga dikembangkan menjadi beberapa variasi antara lain *Proof of Weight (PoW)*, *Proof of Reputatio (PoR)*, *Proof of Space (PoS)*, *Proof of History (PoH)*, *Proof of Burn (PoB)*.

B. Proof of Stake (PoS)

PoS tidak memerlukan node untuk membeli peralatan mahal yang digunakan untuk menambang. Sebuah node dapat melakukan penambangan atau validasi blok berdasarkan pembuktian kepemilikan, yaitu jumlah koin. PoS menyarankan pembelian mata uang kripto kemudian menggunakannya untuk membeli peluang pembuatan blok [57][58]. PoS merupakan protokol konsensus yang didedikasikan untuk open blockchain, keanggotaan terbuka untuk bergabung dengan jaringan. PoS ini mendefinisikan sekelompok validator yang bertugas untuk mengusulkan transaksi berikut untuk dimasukkan ke dalam buku besar (*ledger*) [59][60]. Varian PoS juga dikembangkan oleh komunitas seperti *Peercoin* [61], *Cloakcoin* [62], *Novacoin* [63] dll. PoS juga mempunyai variasi dalam algoritma yaitu *Delegated Proof of Stake (DpoS)* yang digunakan untuk membuat voting dari pemangku kepentingan untuk memilih simpul yang akan dibuat rantai(chain) [64] [65]. Algoritma *DpoS* digunakan untuk meningkatkan throughput transaksi dan kecepatan verifikasi [65].

C. Proof of Existence (PoE)

PoE merupakan sistem untuk memverifikasi keberadaan dokumen atau file tertentu pada waktu tertentu berdasarkan stempel waktu transaksi, fungsinya untuk memberikan informasi kepemilikan data tanpa mengungkapkan data sebenarnya. Model *PoE* ini berguna dalam membuktikan keberadaan dokumen hak cipta, seperti paten.

D. Proof of eXercise (PoX)

PoX merupakan sebuah pendekatan untuk merasionalisasi penambangan dalam mata uang kripto (Bitcoin) berbasis matrik untuk penyelesaian masalah ilmiah pada dunia nyata, Penambang akan memecahkan masalah dengan berbasiskan matrik yang diberikan kepada karyawan didalam sistem [66]. Sebagai contohnya yaitu pengurutan *DNA* dan *RNA* untuk perbandingan data dalam menyelesaikan masalah matrik. Penggunaan matrik didasarkan pada dua hal yaitu 1) Matrik mempunyai sifat komposisi yang menarik dan membantu dalam pengaturan tingkat kesulitan, verifikasi kolaboratif, dan pengumpulan data, 2) Mencakup rentang yang luas terkait masalah dunia nyata dan menjadi abstraksi prinsip pada masalah komputasi ilmiah, diantaranya *DNA* dan *RNA*, oengurutan dan perbandingan data [67][68], analisis struktur protein, perbandingan gambar, superposisi objek, pencocokan permukaan [69][70].

E. Byzantine Fault Tolerance (BFT)

BFT merupakan protokol yang diterapkan untuk menjamin sistem atau aplikasi yang benar sesuai dengan spesifikasinya bahkan jika ada kesalahan sewenang-wenang (*Byzantine Fault*) selama batas ambang tertentu terpenuhi [71][72]. Protokol *BFT* dikategorikan kedalam model jaringan *synchronous*, *asynchronous* atau *partially synchronous* [71], untuk menjadi *BFT*, kontinuitas juga harus dijaga dari kegagalan sewenang-wenang dalam mengikuti protokol. Ketika ada node berkomunikasi dalam sistem, kemudian membuat klaim peristiwa penggabungan beserta informasi yang dimiliki. Kegagalan dalam mengikuti protokol dapat dibagi menjadi tiga yaitu Komunikasi data yang tidak valid, komunikasi data yang tidak autentik, dan komunikasi data autentik yang berbeda yang dikirim ke node yang berbeda [73]. Konsensus diperlukan jika terjadi kehilangan layanan sistem atau kegagalan karena kesalahan byzantium di blockchain, node dalam jaringan harus mencapai konsensus bahkan jika beberapa node gagal merespon dan menjaga konsistensi informasi dalam jaringan blockchain, ini salah satu tantangan sistem distribusi [74]. Untuk memilih skema kontrol akses yang diijinkan dalam fungsionalitas jaringan, *Blockchain* mengadopsi konsensus *BFT* seperti *Practical BFT (PBFT)* [75] untuk mencapai konsensus diantara sekelompok node kecil yang diautentikasi contohnya *Hyperledger Fabric v0.5* [76].

Terdapat tiga algoritma untuk terkait permasalahan *Byzantine fault* yaitu, *Practical Byzantine Fault Tolerance (PBFT)*, *Delegate Byzantine Fault Tolerance (DBFT)*, dan *Sieve Consensus*. *PBFT* merupakan algoritma yang banyak digunakan dan dikembangkan untuk mengatasi masalah *Byzantine faults*. *PBFT* adalah sebuah algoritma untuk mengatasi kesalahan *Byzantine fault*, untuk bertahan secara efisien dari *Byzantine faults* pada jaringan asinkron, kemudian dibuat protokol replikasi mesin pertama [77]. Algoritma ini mencakup tiga bagian yaitu protokol konsensus tiga fase, protokol perubahan, dan mekanisme pos pemeriksaan [78]. *PBFT* lebih cocok untuk rantai konsorsium yang sebagian terdesentralisasi, tahan terhadap node *Byzantine* dan konsistensi yang kuat [79][80].

F. Proof of Luck (PoL)

PoL dikembangkan untuk mengatasi keterbatasan *PoW* yaitu mengurangi daya komputasi saat proses transaksi dan meningkatkan throughput [81]. Algoritma ini berdasarkan pada *TEE (trusted execution environment)*, yang terdiri dari fungsi *PollRound* dan *PollMine*. *TEE* digunakan untuk membangun konsensus primitif yang baru untuk desain mata uang elektronik, Kemampuannya dapat menerapkan pemrosesan yang benar saat operasi kritis dan membatasi efek sybil yang berjalan di bawah satu unit perangkat keras [82]. Nilai 0 dan 1 digunakan sebagai nilai keberuntungan acak untuk setiap blok yang ditambang [11]. Algoritma ini mempunyai kekebalan yang tinggi terhadap serangan double-

spending, tetapi masalah utama protokol ini yaitu ketergantungan pada Intel dan ini bertentangan dengan desentralisasi blockchain [83].

G. Proof of Importance (PoI)

PoI digunakan oleh *NEM/XEM (New Economy Movement)*, ini merupakan mata uang kripto dengan konsep pamanenan yang mirip dengan penambangan dengan menggunakan peringkat setiap akun berdasarkan koin yang sudah diinvestasikan dan belum berbasiskan konsep teori jaringan. *PoI* mengandalkan jumlah koin harian yang ada diakun sebuah node di jaringan untuk memperkirakan kepentingannya [11]. Beberapa keuntungan *PoI* antara lain Efisiensi energi, Menghindari penimbunan koin, Insentif lebih rendah, Mencegah fork.

H. Proof of Elapses Time (PoET)

Algoritma ini memilih blok berikutnya secara adil dan menggunakan sistem ijin blockchain tetapi tidak membutuhkan token. Setiap validator pada sistem mendapat peluang yang masuk wajar untuk membuat bloknnya [60]. Konsep *PoET* menggunakan model pemilu berbasis lotere yang diacak untuk memilih pemimpin baru untuk membuat blok diblockchain. *TEE* digunakan untuk memastikan lingkungan aman dalam proses pemilihan ini. Langkah dalam pemilihan antara lain: Node validator dan penambang menjalankan *TEE (Intel SGX)*, setiap node validator meminta waktu tunggu, node dengan waktu tunggu terpendek akan memenangkan pemilihan untuk menjadi simpul pemimpin [11]. Kelemahan utama yaitu ketergantungan pada perangkat keras [84].

V. IMPLEMENTASI BLOCKCHAIN

Teknologi *Blockchain* tidak hanya digunakan pada sektor keuangan saja, tetapi di era Industri 4.0 dan *Blockchain 3.0*, teknologi ini banyak diterapkan diberbagai sektor.

A. Health Care

Blockchain dapat digunakan untuk menyimpan data kesehatan pasien, sistem ini memungkinkan menyimpan seluruh riwayat kesehatan setiap pasien yang disimpan diblockchain individual [85]. Data yang disimpan pada sistem *data lake*, digunakan sebagai kueri sederhana, analisis tingkat lanjut dan machine learning, *Data lake* merupakan alat sederhana untuk menyimpan berbagai jenis data [86]. Teknologi ini memiliki banyak potensi dalam industri perawatan kesehatan dikarenakan ada kegagalan pertukaran informasi konvensional dan catatan kesehatan pribadi. Industri layanan kesehatan memiliki persyaratan unik seperti *interoperability*, *non-repudiation*, *access control*, *authentication*, *medical data sharing*, dan *mobility*. Di era Industri 4.0, kesehatan data perawatan dikumpulkan dalam bentuk file, sensor yang digunakan, dan aplikasi lainnya [87]. Berikut beberapa penerapan dalam bidang kesehatan:

- 1) *Patient data management*, Blockchain telah digunakan secara luas untuk pengelolaan data pasien terutama untuk meningkatkan keamanan dan efektivitas biaya. Data medis disimpan secara elektronik, janji temu pasien dikelola, penagihan dan rekening ditangani, dan tes laboratorium dilakukan [88].
- 2) *Drug traceability*, untuk menghindari pemalsuan obat digunakan teknologi berbasis blockchain yang memungkinkan peningkatan efisiensi rantai pasokan dengan mencegah penipuan dan produk palsu. Ini dirancang dengan smart contract serta sistem pelacakan obat [89].
- 3) *Cryptocurrency payments*, beberapa manfaat pembayaran mata uang kripto dalam layanan kesehatan yaitu penggunaan blockchain, buku besar (ledger) melacak semua transaksi. Data yang disimpan berisi semua informasi tentang pemilik koin. Blockchain memungkinkan pasien untuk melakukan pertukaran [90].
- 4) *Clinical trials* dan *data security*, dalam studi klinis, penting untuk mengumpulkan data yang otentik dan benar. Hal ini penting untuk mengkorelasikan, mengukur, dan membuat analisis. Hal ini menambah lapisan keselamatan dan keamanan pada informasi identitas pribadi dan sensitif yang dikhawatirkan oleh pasien jika informasi tersebut dibobol di lokasi di mana pencurian identitas dapat terjadi [87].
- 5) *Device tracking*, Cara penting lainnya untuk merevolusi layanan kesehatan adalah dengan melacak perangkat medis mulai dari produksi hingga penghentian penggunaan. Semua rumah sakit kesulitan mengelola kumpulan peralatan medis yang digunakan oleh banyak departemen dan pasien [91].
- 6) *Healthcare internet of things (IoT)*, Teknologi *Blockchain* untuk industri kesehatan mempunyai potensi untuk meningkatkan keamanan dan transparansi data *IoT* sekaligus memungkinkan efisiensi, skalabilitas, dan standarisasi *IoT* di masa depan [92].

B. Smart City

Tantangan utama yang menghambat perkembangan *smart city* bukan diteliti tetapi pada data yang dihasilkan oleh teknologi tersebut dan bagaimana cara menjaga keamanannya. Salah satu caranya menggunakan *Blockchain*, teknologi *Blockchain* berperan karena berpotensi memberikan keamanan [93]. Teknologi ini memungkinkan pemerintah daerah untuk menyederhanakan data kota dan membuatnya tidak mudah untuk diretas. Blockchain, jika digabungkan dengan teknologi big data, dapat memungkinkan banyak pihak untuk berinteraksi secara kooperatif. Hal ini dapat membantu pemerintah kota mencapai tujuan ekonomi digital mereka sekaligus memastikan keamanan jaringan yang maksimal. Komponen yang termasuk *smart city* antara lain *smart people*, *smart governance*, *smart homes*, *smart infrastructure*, *smart technology*, *smart economy*, *smart mobility*, *smart living*,

smart parking, *smart factory*, *smart health*, *smart tourism*, dan *smart environment* [94].

C. Transportation Management

Aliran data real-time yang konstan seperti posisi kendaraan, kecepatan, pemecahan, percepatan dan lintasan dikumpulkan merupakan beberapa hal yang harus diperhatikan dalam mengatur transportasi, data tersebut harus terintegrasi antara kendaraan dan infrastruktur pengelolaan transportasi. *Blockchain* dapat memfasilitasi komunikasi antara kendaraan dan infrastruktur dengan pertukaran data yang dianggap sebagai transaksi untuk disimpan dan diambil dari *database Blockchain*. Salah satu perhatian utama terkait kendaraan baru yang terhubung adalah keselamatan dan keamanan komunikasi yang terkait erat dengan keselamatan lalu lintas. Ketika aliran data langsung dihasilkan oleh kendaraan yang terhubung dan otonom, *desentralisasi*, *heterogenitas*, dan ketidakpercayaan dari *Vehicle-to-Vehicle (V2V)* dan *Vehicle-to-Everything (V2X)* akan menimbulkan tantangan dalam mengamankan pesan yang dikirimkan dan eksekusi transaksi [95]. Untuk mengatasi hal tersebut, *Blockchain* sebagai database yang susah untuk dirusak dapat dijadikan solusi [96] yaitu dengan mengintegrasikan *Blockchain* dengan *V2V* dan *V2X* [97]. Selain itu, pada kendaraan listrik dan hibrida, *Blockchain* dapat digunakan untuk melindungi interaksi energi dan informasi antara kendaraan listrik dan hibrida dalam *smart grid* [98][99].

D. Agriculture

Teknologi modern banyak diterapkan pada sektor pertanian dengan menggunakan perangkat nirkabel untuk meningkatkan produktivitas pertanian dan pengelolaan biaya [100]. Pertanian yang presisi menggunakan perangkat IoT untuk penginderaan jarak jauh dan memantau kondisi tanaman pada berbagai tahap pertumbuhan [101][102]. Data pertanian yang dikirim melalui nirkabel harus terjamin sistem keamanannya, *Blockchain* digunakan sebagai pusat IoT untuk mengumpulkan data dan menggunakan *smart contract* untuk mengontrol interaksi diantara para pemangku kepentingan [103]. *Blockchain* mempunyai karakter *immutable*, *available*, *transparent*, dan aman di bidang pertanian, serta mempunyai mekanisme kuat dalam mengintegrasikan *Blockchain*, *smart contract*, dan jaringan *IoT*.

Integrasi *smart contract*, *Blockchain* dan *IoT*, telah terbukti sebagai tindakan yang cerdas, aman, dan andal untuk melacak dan memantau proses dan operasi [103]. Teknologi *Blockchain* diakui sebagai buku besar (*ledger*) dibidang pertanian untuk mencatat semua transaksi keuangan dan informasi yang diperlukan dan dibagikan oleh petani kepada pelanggan disemua tingkatan [104]. *Blockchain* digunakan untuk meningkatkan rantai pasokan makanan, penelusuran polutan, keamanan makanan, dan sistem yang transparan, sedangkan untuk memantau pengendalian hama, ketinggian air, dan kondisi lingkungan dari degradasi lingkungan digunakan sensor dan IoT [105][106]. *Smart agriculture* menggabungkan berbagai teknologi diantara perangkat IoT, sensor dan drone

yang mengumpulkan data tentang kelembaban tanah, suhu, kelembaban, dan faktor lingkungan lainnya. *Smart agriculture* membantu mengurangi penggunaan bahan kimia dan pupuk berbahaya, meningkatkan kesehatan tanah, dan mengurangi polusi [107]. Integrasi IoT dengan *Blockchain* digunakan untuk mengamankan sistem pertanian dan untuk mengoptimalkan produksi pertanian [108].

VI. DISKUSI

Perkembangan teknologi Blockchain pada era Industri 4.0 menunjukkan bahwa teknologi ini tidak hanya digunakan pada sistem cryptocurrency, tetapi juga telah berkembang menjadi solusi untuk meningkatkan keamanan, transparansi, integritas, dan efisiensi pertukaran data di berbagai sektor. Implementasi Blockchain pada bidang keuangan, kesehatan, logistik, pemerintahan, pendidikan, hingga *Internet of Things (IoT)* memperlihatkan bahwa teknologi desentralisasi memiliki potensi besar dalam mendukung sistem digital yang lebih aman dan terpercaya. Selain menyediakan mekanisme penyimpanan data terdistribusi, Blockchain juga mampu mendukung penerapan *smart contract* dan *decentralized applications (DApps)* yang memungkinkan otomatisasi layanan digital pada berbagai platform industri. Namun demikian, penerapan Blockchain masih menghadapi beberapa tantangan, seperti skalabilitas jaringan, tingginya konsumsi energi pada mekanisme konsensus tertentu, interoperabilitas antarplatform, serta regulasi dan privasi data. Seiring dengan perkembangan teknologi, Blockchain juga memiliki peluang untuk diintegrasikan dengan teknologi lain seperti *Artificial Intelligence (AI)*, *cloud computing*, *big data*, dan *IoT* guna membangun sistem industri yang lebih cerdas dan otomatis. Oleh karena itu, pengembangan algoritma konsensus dan arsitektur Blockchain yang lebih efisien, aman, dan adaptif menjadi salah satu fokus penting dalam penelitian Blockchain di masa depan. Kajian ini memberikan gambaran mengenai perkembangan teknologi Blockchain beserta implementasinya di berbagai sektor sehingga dapat menjadi referensi dalam pengembangan sistem digital berbasis Blockchain pada era Industri 4.0.

VII. KESIMPULAN

Blockchain merupakan teknologi terdistribusi yang berkembang pesat dan memiliki peran penting dalam mendukung transformasi digital di era Industri 4.0. Teknologi ini mampu meningkatkan keamanan, transparansi, integritas, dan privasi data melalui mekanisme desentralisasi dan algoritma konsensus yang diterapkan pada berbagai platform Blockchain. Kajian ini membahas evolusi Blockchain mulai dari generasi *cryptocurrency*, *smart contract*, hingga *decentralized applications (DApps)*, beserta perkembangan arsitektur, tipe akses data, dan mekanisme konsensus yang digunakan. Hasil kajian menunjukkan bahwa setiap jenis Blockchain, baik *public*, *private*, maupun *consortium*,

memiliki karakteristik, keunggulan, dan tantangan implementasi yang berbeda sesuai kebutuhan organisasi dan sektor industri. Selain itu, pengembangan mekanisme konsensus seperti *Proof of Work (PoW)*, *Proof of Stake (PoS)*, dan model konsensus lainnya terus dilakukan untuk meningkatkan efisiensi, skalabilitas, dan keamanan sistem Blockchain. Implementasi Blockchain telah diterapkan secara luas pada berbagai sektor, seperti keuangan, kesehatan, pendidikan, logistik, pemerintahan, serta *Internet of Things (IoT)*. Meskipun demikian, masih terdapat beberapa tantangan dalam implementasinya, antara lain konsumsi energi, skalabilitas jaringan, interoperabilitas antarplatform, regulasi, serta keamanan dan privasi data. Oleh karena itu, penelitian dan pengembangan Blockchain di masa depan diharapkan dapat berfokus pada peningkatan efisiensi algoritma konsensus dan integrasi *Blockchain* dengan teknologi Industri 4.0 lainnya seperti *Artificial Intelligence (AI)*, *cloud computing*, dan *IoT*. Kajian ini diharapkan dapat menjadi referensi akademik dan praktis dalam memahami perkembangan teknologi Blockchain serta peluang implementasinya pada berbagai sektor di era Industri 4.0, sekaligus menjadi dasar bagi pengembangan penelitian lanjutan terkait optimalisasi Blockchain yang lebih adaptif, efisien, dan aman.

REFERENSI

- [1] N. Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," *SSRN Electron. J.*, pp. 1–9, 2022, doi: 10.2139/ssrn.3977007.
- [2] M. M. Nuttah, P. Roma, G. Lo Nigro, and G. Perrone, "Understanding blockchain applications in Industry 4.0: From information technology to manufacturing and operations management," *J. Ind. Inf. Integr.*, vol. 33, no. March, 2023, doi: 10.1016/j.jii.2023.100456.
- [3] M. Javaid, A. Haleem, R. Pratap Singh, S. Khan, and R. Suman, "Blockchain technology applications for Industry 4.0: A literature-based review," *Blockchain Res. Appl.*, vol. 2, no. 4, 2021, doi: 10.1016/j.bcr.2021.100027.
- [4] Q. Bao, B. Li, T. Hu, and X. Sun, "A survey of blockchain consensus safety and security: State-of-the-art, challenges, and future work," *J. Syst. Softw.*, vol. 196, 2023, doi: 10.1016/j.jss.2022.111555.
- [5] S. A. Sarkodie, M. Y. Ahmed, and P. A. Owusu, "COVID-19 pandemic improves market signals of cryptocurrencies—evidence from Bitcoin, Bitcoin Cash, Ethereum, and Litecoin," *Financ. Res. Lett.*, vol. 44, no. April 2021, 2022, doi: 10.1016/j.frl.2021.102049.
- [6] W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li, and R. Chen, "NutBaaS: A Blockchain-As-A-Service Platform," *IEEE Access*, vol. 7, pp. 134422–134433, 2019, doi: 10.1109/ACCESS.2019.2941905.
- [7] E. Callens, "Financial instruments entail liabilities: Ether, bitcoin, and litecoin do not," *Comput. Law Secur. Rev.*, vol. 40, no. July 2020, pp. 1–20, 2021, doi: 10.1016/j.clsr.2020.105494.
- [8] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Futur. Gener. Comput. Syst.*, vol. 107, pp. 841–853, 2020, doi: 10.1016/j.future.2017.08.020.
- [9] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: A survey on applications and security privacy Challenges," *Internet of Things (Netherlands)*, vol. 8, 2019, doi: 10.1016/j.iot.2019.100107.
- [10] N. Tapus and A. Manolache, "ScienceDirect Integrated Decision Making Making using using the the Blockchain Blockchain Integrated Decision," no. Itqm 2019, 2020.
- [11] M. Nasir, M. Bhutta, A. A. Khwaja, A. Nadeem, and H. F. Ahmad, "A Survey on Blockchain Technology: Evolution, Architecture and Security," vol. 9, 2021, doi: 10.1109/ACCESS.2021.3072849.
- [12] Y. Xu, "Segment Blockchain: A Size Reduced Storage Mechanism for Blockchain," vol. 8, 2020.
- [13] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016,

- doi: 10.1109/ACCESS.2016.2566339.
- [14] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger," *Ethereum Proj. Yellow Pap.*, pp. 1–32, 2014.
 - [15] T. Hewa, M. Ylianttila, and M. Liyanage, "Survey on blockchain based smart contracts: Applications, opportunities and challenges," *J. Netw. Comput. Appl.*, vol. 177, no. November 2020, 2021, doi: 10.1016/j.jnca.2020.102857.
 - [16] N. Atzei, M. Bartoletti, T. Cimoli, S. Lande, and R. Zunino, "SoK: Unraveling bitcoin smart contracts," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10804 LNCS, pp. 217–242, 2018, doi: 10.1007/978-3-319-89722-6_9.
 - [17] M. Bartoletti and L. Pompianu, "An Empirical analysis of smart contracts: Platforms, applications, and design patterns," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10323 LNCS, pp. 494–509, 2017, doi: 10.1007/978-3-319-70278-0_31.
 - [18] N. F. Samreen and M. H. Alalfi, "An empirical study on the complexity, security and maintainability of Ethereum-based decentralized applications (DApps)," *Blockchain Res. Appl.*, vol. 4, no. 2, 2023, doi: 10.1016/j.bcr.2022.100120.
 - [19] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A Survey of Distributed Consensus Protocols for Blockchain Networks," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020, doi: 10.1109/COMST.2020.2969706.
 - [20] J. Kehrl, "Blockchain 2.0-From Bitcoin Transactions to Smart Contract applications," pp. 1–37, 2016.
 - [21] Melanie Swan, *Blockchain Blueprint for a New Economy*, 1st ed. United States of America: O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2015.
 - [22] H. Taherdoost, "Smart Contracts in Blockchain Technology: A Critical Review," *Inf.*, vol. 14, no. 2, 2023, doi: 10.3390/info14020117.
 - [23] M. S. Alnahari and S. T. Ariaratnam, "The Application of Blockchain Technology to Smart City Infrastructure," *Smart Cities*, vol. 5, no. 3, pp. 979–993, 2022, doi: 10.3390/smartcities5030049.
 - [24] W. Kozłowski and K. Suwar, "Smart City: Definitions, Dimensions, and Initiatives," *Eur. Res. Stud. J.*, vol. XXIV, no. Special Issue 3, pp. 509–520, 2021, doi: 10.35808/ersj/2442.
 - [25] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, "Decentralized Applications: The Blockchain-Empowered Software System," *IEEE Access*, vol. 6, no. September, pp. 53019–53033, 2018, doi: 10.1109/ACCESS.2018.2870644.
 - [26] E. Nkurunziza, T. Lawrence, E. Issameldeen, and G. Mwitende, "AP-HBSG: Authentication protocol for heterogeneous blockchain-based smart grid environment," *Comput. Commun.*, vol. 212, no. January, pp. 212–226, 2023, doi: 10.1016/j.comcom.2023.09.034.
 - [27] J. Gao *et al.*, "GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid," *IEEE Access*, vol. 6, no. March, pp. 9917–9925, 2018, doi: 10.1109/ACCESS.2018.2806303.
 - [28] Y. Li, R. Rahmani, N. Fouassier, P. Stenlund, and K. Ouyang, "A blockchain-based architecture for stable and trustworthy smart grid," *Procedia Comput. Sci.*, vol. 155, no. 2018, pp. 410–416, 2019, doi: 10.1016/j.procs.2019.08.057.
 - [29] L. Xu, M. Lin, Y. Feng, and Y. Sun, "BPDST: Blockchain-Based Privacy-Preserving Data Sharing on Thin Client for Electronic Medical Records," *J. Comput. Inf. Technol.*, vol. 29, no. 4, pp. 235–250, 2022, doi: 10.20532/CIT.2021.1005412.
 - [30] L. Zhang, M. Peng, W. Wang, Y. Su, S. Cui, and S. Kim, "Secure and efficient data storage and sharing scheme based on double blockchain," *Comput. Mater. Contin.*, vol. 66, no. 1, pp. 499–515, 2021, doi: 10.32604/cmc.2020.012205.
 - [31] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Inf.*, vol. 8, no. 2, 2017, doi: 10.3390/info8020044.
 - [32] N. Zeinali, A. Asosheh, and S. Setareh, "The conceptual model to solve the problem of interoperability in health information systems," *2016 8th Int. Symp. Telecommun. IST 2016*, no. September 2016, pp. 684–689, 2017, doi: 10.1109/ISTEL.2016.7881909.
 - [33] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of Blockchains in the Internet of Things: A Comprehensive Survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019, doi: 10.1109/COMST.2018.2886932.
 - [34] L. Xu *et al.*, "Enabling the Sharing Economy: Privacy Respecting Contract based on Public Blockchain," *BCC 2017 - Proc. ACM Work. Blockchain, Cryptocurrencies Contract. co-located with ASIA CCS 2017*, no. October, pp. 15–21, 2017, doi: 10.1145/3055518.3055527.
 - [35] Q. Wang and Y. Liu, "Blockchain for Public Safety: A Survey of Techniques and Applications," *J. Saf. Sci. Resil.*, 2023, doi: 10.1016/j.jnlssr.2023.09.001.
 - [36] V. Gugueoth, S. Safavat, S. Shetty, and D. Rawat, "A review of IoT security and privacy using decentralized blockchain techniques," *Comput. Sci. Rev.*, vol. 50, 2023, doi: 10.1016/j.cosrev.2023.100585.
 - [37] Z. Ullah, M. Naeem, A. Coronato, P. Ribino, and G. De Pietro, "Blockchain Applications in Sustainable Smart Cities," *Sustain. Cities Soc.*, vol. 97, no. June, p. 104697, 2023, doi: 10.1016/j.scs.2023.104697.
 - [38] B. Godavarthi, M. Dhar, S. A. Devi, S. S. Raju, A. Balaram, and G. Srilakshmi, "Blockchain integration with the internet of things for the employee performance management," *J. High Technol. Manag. Res.*, vol. 34, no. 2, p. 100468, 2023, doi: 10.1016/j.hitech.2023.100468.
 - [39] M. M. Nuttah, P. Roma, G. Lo Nigro, and G. Perrone, "Journal of Industrial Information Integration Understanding blockchain applications in Industry 4.0: From information technology to manufacturing and operations management," *J. Ind. Inf. Integr.*, vol. 33, no. March, p. 100456, 2023, doi: 10.1016/j.jii.2023.100456.
 - [40] T. A. Almeshal, "Blockchain for Businesses: A Scoping Review of Suitability Evaluations Frameworks," *IEEE Access*, vol. 9, pp. 155425–155442, 2021, doi: 10.1109/ACCESS.2021.3128608.
 - [41] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, 2018, doi: 10.1504/IJWGS.2018.095647.
 - [42] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K. L. Tan, "BLOCKBENCH: A framework for analyzing private blockchains," *Proc. ACM SIGMOD Int. Conf. Manag. Data*, vol. Part F1277, pp. 1085–1100, 2017, doi: 10.1145/3035918.3064033.
 - [43] X. Xu, Y. Guo, and Y. Guo, "Fog-enabled private blockchain-based identity authentication scheme for smart home," *Comput. Commun.*, vol. 205, no. February 2022, pp. 58–68, 2023, doi: 10.1016/j.comcom.2023.04.005.
 - [44] R. Yang *et al.*, "Public and private blockchain in construction business process and information integration," *Autom. Constr.*, vol. 118, no. May, p. 103276, 2020, doi: 10.1016/j.autcon.2020.103276.
 - [45] E. Ben Hamida, K. L. Brousmiche, H. Levard, and E. Thea, "Blockchain for Enterprise: Overview, Opportunities and Challenges," *13th Int. Conf. Wirel. Mob. Commun.*, no. June, p. 7, 2017.
 - [46] Y. Chen *et al.*, "Decentralized data access control over consortium blockchains," *Inf. Syst.*, vol. 94, p. 101590, 2020, doi: 10.1016/j.is.2020.101590.
 - [47] Z. Fu, P. Dong, and Y. Ju, "An intelligent electric vehicle charging system for new energy companies based on consortium blockchain," *J. Clean. Prod.*, vol. 261, p. 121219, 2020, doi: 10.1016/j.jclepro.2020.121219.
 - [48] Z. Yu, D. Xue, J. Fan, and C. Guo, "DNSTSM: DNS Cache Resources Trusted Sharing Model Based on Consortium Blockchain," *IEEE Access*, vol. 8, pp. 13640–13650, 2020, doi: 10.1109/ACCESS.2020.2966428.
 - [49] A. Montresor, "Practical Byzantine Fault Tolerance," no. April 2001, 2016.
 - [50] M. He *et al.*, "T2L: A traceable and trustable consortium blockchain for logistics," *Digit. Commun. Networks*, 2022, doi: 10.1016/j.dcan.2022.06.015.
 - [51] K. Hasan, M. J. M. Chowdhury, K. Biswas, K. Ahmed, M. S. Islam, and M. Usman, "A blockchain-based secure data-sharing framework for Software Defined Wireless Body Area Networks," *Comput. Networks*, vol. 211, no. April, p. 109004, 2022, doi: 10.1016/j.comnet.2022.109004.
 - [52] H. Guo and X. Yu, "Blockchain: Research and Applications A survey on blockchain technology and its security," *Blockchain Res. Appl.*, vol. 3, no. 2, p. 100067, 2022, doi: 10.1016/j.bcr.2022.100067.
 - [53] D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. Njilla, "Consensus protocols for blockchain-based data provenance: Challenges and opportunities," *2017 IEEE 8th Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. UEMCON 2017*, vol. 2018–Janua, no. October, pp. 469–474, 2017, doi: 10.1109/UEMCON.2017.8249088.
 - [54] J. Truby, "Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies," *Energy Res. Soc. Sci.*, vol. 44, no. July, pp. 399–410, 2018, doi: 10.1016/j.erss.2018.06.009.
 - [55] N. Christin and R. Safavi-Naini, "Majority is not Enough: Bitcoin Mining is Vulnerable* Ittay," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8437, no. March, 2014, doi: 10.1007/978-3-662-45472-5.
 - [56] J. Göbel, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor, "Bitcoin

- blockchain dynamics: The selfish-mine strategy in the presence of propagation delay," *Perform. Eval.*, vol. 104, pp. 23–41, 2016, doi: 10.1016/j.peva.2016.07.001.
- [57] P. Vasin, "BlackCoin's Proof-of-Stake Protocol v2 Pavel," *Self-published*, p. 2, 2014, [Online]. Available: <https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf>.
- [58] A. Kiyaiyas, A. Russell, B. David, and R. Oliynykov, *Ouroboros: A provably secure proof-of-stake blockchain protocol*, vol. 10401 LNCS, no. May. 2017.
- [59] J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartenstein, and J. Herrera-Joancomartí, "Securing Proof-of-Stake Blockchain Protocols Wenting," *Proceedings*, no. September, 2017, doi: 10.1007/978-3-319-67816-0.
- [60] M. Parmar, N. Kumar, H. J. Kaur, A. Sharma, S. Sharma, and M. Sandhu, "Analysis and comparison of different blockchain algorithms in IoT security," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1022, no. 1, 2021, doi: 10.1088/1757-899X/1022/1/012059.
- [61] S. N. Sunny King, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," *Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS'16*, vol. 1919, no. January, pp. 1–27, 2017, [Online]. Available: http://peerco.in/assets/paper/peercoin-paper.pdf%0Ahttp://fc17.ifca.ai/preproceedings/paper_73.pdf%0Ahttp://arxiv.org/abs/1606.06530%0Ahttps://papers.ssrn.com/sol3/papers.cfm?abstract_id=2977811%0Ahttp://dl.acm.org/citation.cfm?doid=2976749.2978389%0Ahttp.
- [62] S. Ahmed, K. Grobys, and N. Sapkota, "Profitability of technical trading rules among cryptocurrencies with privacy function," *Financ. Res. Lett.*, vol. 35, no. February, p. 101495, 2020, doi: 10.1016/j.frl.2020.101495.
- [63] T. Papadimitriou, P. Gogas, and F. Gkatzoglou, "The evolution of the cryptocurrencies market: A complex networks approach," *J. Comput. Appl. Math.*, vol. 376, p. 112831, 2020, doi: 10.1016/j.cam.2020.112831.
- [64] M. Borse, P. Shendkar, Y. Undre, A. Mahadik, and R. Y. Patil, "A Review of Blockchain Consensus Algorithm," *Lect. Notes Networks Syst.*, vol. 444, pp. 415–426, 2022, doi: 10.1007/978-981-19-2500-9_31.
- [65] Y. Sun, B. Yan, Y. Yao, and J. Yu, "DT-DPoS: A Delegated Proof of Stake Consensus Algorithm with Dynamic Trust," *Procedia Comput. Sci.*, vol. 187, pp. 371–376, 2021, doi: 10.1016/j.procs.2021.04.113.
- [66] A. Shoker, "Brief announcement: Sustainable blockchains through proof of eExercise," *Proc. Annu. ACM Symp. Princ. Distrib. Comput.*, no. July 2018, pp. 269–271, 2018, doi: 10.1145/3212734.3212781.
- [67] A. Abboud, V. V. Williams, and O. Weimann, "Consequences of faster alignment of sequences," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8572 LNCS, no. PART 1, pp. 39–51, 2014, doi: 10.1007/978-3-662-43948-7_4.
- [68] P. Bille, "A survey on tree edit distance and related problems," *Theor. Comput. Sci.*, vol. 337, no. 1–3, pp. 217–239, 2005, doi: 10.1016/j.tcs.2004.12.030.
- [69] H. ALT and M. GODAU, "Computing the Fréchet Distance Between Two Polygonal Curves," *Int. J. Comput. Geom. Appl.*, vol. 5, no. 01n02, pp. 75–91, 1995, doi: 10.1142/s0218195995000064.
- [70] M. M. Deza and E. Deza, *Encyclopedia of distances*. 2009.
- [71] T. Freitas, J. Soares, M. E. Correia, and R. Martins, "Deterministic or probabilistic? - A survey on Byzantine fault tolerant state machine replication," *Comput. Secur.*, vol. 129, 2023, doi: 10.1016/j.cose.2023.103200.
- [72] L. Lamport, "Time, Clocks, and the Ordering of Events in a Distributed System," *Commun. ACM*, vol. 21, no. 7, pp. 558–565, 1978, doi: 10.1145/359545.359563.
- [73] R. Arnold and D. Longley, "Continuity: A deterministic Byzantine fault tolerant asynchronous consensus algorithm," *Comput. Networks*, vol. 199, 2021, doi: 10.1016/j.comnet.2021.108431.
- [74] W. Wang *et al.*, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access*, vol. 7, no. January, pp. 22328–22370, 2019, doi: 10.1109/ACCESS.2019.2896108.
- [75] A. Montresor, "Distributed Algorithms Practical Byzantine Fault Tolerance," no. April 2001, 2016.
- [76] C. Cachin, S. Schubert, and M. Vukolić, "Architecture of the Hyperledger Blockchain Fabric," *Leibniz International Proceedings in Informatics, LIPIcs*, vol. 70, p. 24.1-24.16, 2017, doi: 10.4230/LIPIcs.OPODIS.2016.24.
- [77] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, 2002, doi: 10.1145/571637.571640.
- [78] Y. Wu, L. Wu, and H. Cai, "Reinforced practical Byzantine fault tolerance consensus protocol for cyber physical systems," *Comput. Commun.*, vol. 203, no. August 2022, pp. 238–247, 2023, doi: 10.1016/j.comcom.2023.03.016.
- [79] Y. Chen *et al.*, "An improved algorithm for practical byzantine fault tolerance to large-scale consortium chain," *Inf. Process. Manag.*, vol. 59, no. 2, pp. 1–15, 2022, doi: 10.1016/j.ipm.2022.102884.
- [80] H. Qin, Y. Cheng, X. Ma, F. Li, and J. Abawajy, "Weighted Byzantine Fault Tolerance consensus algorithm for enhancing consortium blockchain efficiency and security," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 10, pp. 8370–8379, 2022, doi: 10.1016/j.jksuci.2022.08.017.
- [81] Y. Zhang, B. Yan, Y. Yao, and J. Yu, "Proof of Random Trust Consensus Mechanism for Power Resource Sharing System," *Procedia Comput. Sci.*, vol. 187, pp. 402–407, 2021, doi: 10.1016/j.procs.2021.04.079.
- [82] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of Luck: An efficient blockchain consensus protocol," *SysTEX 2016 - 1st Work. Syst. Softw. Trust. Exec. Coloca. with ACM/IFIP/USENIX Middlew. 2016*, pp. 2–7, 2016, doi: 10.1145/3007788.3007790.
- [83] J. Yusoff, Z. Mohamad, and M. Anuar, "A Review: Consensus Algorithms on Blockchain," *J. Comput. Commun.*, vol. 10, no. 9, pp. 37–50, 2022, doi: 10.4236/jcc.2022.109003.
- [84] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (PoET)," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10616 LNCS, no. May 2019, pp. 282–297, 2017, doi: 10.1007/978-3-319-69084-1_19.
- [85] S. Singh and A. S. M. S. Hosen, "Blockchain Security Attacks , Challenges, and Solutions for the Future Distributed IoT Network," vol. 9, 2021, doi: 10.1109/ACCESS.2021.3051602.
- [86] Y. Sun, Y. Yuan, Q. Wang, L. Wang, E. Li, and L. Qiao, "Research on the Signal Reconstruction of the Phased Array Structural Health Monitoring Based Using the Basis Pursuit Algorithm," vol. 58, no. 2, pp. 409–420, 2019, doi: 10.32604/cmc.2019.03642.
- [87] J. Andrew, D. Priya, K. M. Sagayam, B. Bhushan, Y. Sei, and J. Eunice, "Journal of Network and Computer Applications Blockchain for healthcare systems: Architecture , security challenges , trends and future directions," *J. Netw. Comput. Appl.*, vol. 215, no. April, p. 103633, 2023, doi: 10.1016/j.jnca.2023.103633.
- [88] A. Shahnaaz, U. Qamar, and A. Khalid, "Using Blockchain for Electronic Health Records," *IEEE Access*, vol. 7, pp. 147782–147795, 2019, doi: 10.1109/ACCESS.2019.2946373.
- [89] A. Musamih *et al.*, "A blockchain-based approach for drug traceability in healthcare supply chain," *IEEE Access*, vol. 9, no. January, pp. 9728–9743, 2021, doi: 10.1109/ACCESS.2021.3049920.
- [90] C. Kombe, M. Ally, and A. Sam, "A review on healthcare information systems and consensus protocols in blockchain technology," *Int. J. Adv. Technol. Eng. Explor.*, vol. 5, no. 49, pp. 473–483, 2018, doi: 10.19101/ijatee.2018.547023.
- [91] R. Jafri and S. Singh, *Blockchain applications for the healthcare sector: Uses beyond Bitcoin*. Elsevier Inc., 2022.
- [92] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Futur. Gener. Comput. Syst.*, vol. 88, no. 2018, pp. 173–190, 2018, doi: 10.1016/j.future.2018.05.046.
- [93] M. N. O. Sadiku *et al.*, "Blockchain in Smart Cities," vol. 7, no. 4, pp. 325–327, 2020.
- [94] V. Albino, U. Berardi, and R. M. Dangelico, "Smart cities: Definitions, dimensions, performance, and initiatives," *J. Urban Technol.*, vol. 22, no. 1, pp. 3–21, 2015, doi: 10.1080/10630732.2014.942092.
- [95] H. N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A Survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, 2019, doi: 10.1109/JIOT.2019.2920987.
- [96] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, 2017, doi: 10.1109/MCOM.2017.1700879.
- [97] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, 2019, doi: 10.1109/JIOT.2018.2836144.
- [98] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling Localized Peer-to-Peer Electricity Trading among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains," *IEEE Trans. Ind. Informatics*, vol. 13, no. 6, pp. 3154–3164, 2017, doi: 10.1109/TII.2017.2709784.
- [99] J. Kang *et al.*, "Blockchain for secure and efficient data sharing in

- vehicular edge computing and networks,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, 2019, doi: 10.1109/JIOT.2018.2875542.
- [100] T. Saba, A. Rehman, K. Haseeb, S. Ali, and J. Lloret, “Trust-based decentralized blockchain system with machine learning using Internet of agriculture things,” vol. 108, no. May 2022, 2023.
- [101] U. Shafi, R. Mumtaz, J. García-Nieto, S. A. Hassan, S. A. R. Zaidi, and N. Iqbal, “Precision agriculture techniques and practices: From considerations to applications,” *Sensors (Switzerland)*, vol. 19, no. 17, pp. 1–25, 2019, doi: 10.3390/s19173796.
- [102] L. Garcia *et al.*, “Deployment strategies of soil monitoring wsn for precision agriculture irrigation scheduling in rural areas,” *Sensors*, vol. 21, no. 5, pp. 1–30, 2021, doi: 10.3390/s21051693.
- [103] T. H. Pranto, A. A. Noman, A. Mahmud, and A. B. Haque, “Blockchain and smart contract for IoT enabled smart agriculture,” *PeerJ Comput. Sci.*, vol. 7, pp. 1–29, 2021, doi: 10.7717/PEERJ-CS.407.
- [104] K. Chatterjee, A. Singh, and Neha, “A blockchain-enabled security framework for smart agriculture,” *Comput. Electr. Eng.*, vol. 106, no. May 2022, 2023, doi: 10.1016/j.compeleceng.2023.108594.
- [105] T. Ahmed, C. L. Karmaker, S. B. Nasir, M. A. Moktadir, and S. K. Paul, “Modeling the artificial intelligence-based imperatives of industry 5.0 towards resilient supply chains: A post-COVID-19 pandemic perspective,” *Comput. Ind. Eng.*, vol. 177, no. January, 2023, doi: 10.1016/j.cie.2023.109055.
- [106] M. W. Akram, N. Akram, W. Hongshu, S. Andleeb, K. Ur Rehman, and F. Hassan, “Investigating the leading drivers of organic farming: A survival analysis,” *Cienc. Rural*, vol. 52, no. 7, 2022, doi: 10.1590/0103-8478CR20200781.
- [107] H. Y. Chen, K. Sharma, C. Sharma, and S. Sharma, “Integrating explainable artificial intelligence and blockchain to smart agriculture: Research prospects for decision making and improved security,” *Smart Agric. Technol.*, vol. 6, no. October, 2023, doi: 10.1016/j.atech.2023.100350.
- [108] K. U. Rehman, S. Andleeb, M. Ashfaq, N. Akram, and M. W. Akram, “Blockchain-enabled smart agriculture: Enhancing data-driven decision making and ensuring food security,” *J. Clean. Prod.*, vol. 427, no. June, p. 138900, 2023, doi: 10.1016/j.jclepro.2023.138900.