JEEEIT TRANSACTIONS, Vol.2,No.1,December 2025

Data explosion of Blockchain-Based Tracking and Tracing Systems: A Review

Mohamed Mostafa Montaser[1], Rasha Ridha Alhanash[2], Ahlam Elmghirbi[1], Salim Tahir Alakari[1], Maisun Alzorgani[1], Osama Salem shtewi[1], Mostafa Nser Brka[1], and Asad Dughman[1]

[1]Department of Information Technology, Higher Institute of Science & Technology –AlShomokh, Tripoli, Libya
[2]National Oil Corporation - Libya

Corresponding author: (DR.MM.MONTASER@GMAIL.COM).

ABSTRACT Blockchain technology enables secure and transparent information exchange within decentralized environments. Its distributed architecture and continuous protocol improvements help streamline validation processes while supporting network scalability. In blockchain systems, transaction verification relies on digital information units recorded across distributed ledgers. However, this design inherently leads to growing data accumulation over time, as historical transactions must be preserved permanently. This data growth creates significant challenges for storage-dependent applications, particularly tracking and tracing systems, where real-time location monitoring and product authentication generate massive datasets. The resulting storage costs also affect other blockchain-enabled services, including video recognition and artificial intelligence applications, which often underperform when deployed on conventional hardware within tracking environments. This review paper examines blockchain's operational framework, exploring its fundamental concepts, classification schemes, underlying principles, and practical implementations in tracking and tracing contexts. The primary focus is addressing data proliferation issues within blockchain networks, specifically as they relate to tracking and tracing systems. Additionally, this study provides a thorough analysis of existing research contributions in this domain.

KEYWORDS blockchain; Tracking; Tracing; Data Explosion; Data Size.

I. INTRODUCTION

Blockchain is considered a new type of database capable of storing information traditionally managed by conventional database systems. It functions by organizing data into a series of interconnected blocks, each linked to the next through a cryptographic reference called a hash. When a new block is created and added to the system, it is connected to the preceding block via this hash reference, forming an unbreakable chain of records. In this decentralized architecture, all blocks are stored and distributed across the network, ensuring that every user and node can access and maintain copies of the blockchain's information [1]. This distributed copy of information is known as the transaction ledger. Consequently, numerous research studies across various disciplines have leveraged blockchain's operational framework to address domain-specific challenges. Notable application areas include information security systems [2], supply chain management [3], digital finance [4], computer networks and applications [5], smart grids and energy [6], Internet of Things (IoT) [7]. These diverse implementations demonstrate blockchain's potential to enhance operational performance and security across a wide spectrum of applications.

II. Blockchain Technology related Applications

Blockchain technology offers numerous practical applications and services across various sectors [8]. Key implementation domains include e-commerce platforms [9] , cloud computing [10], gaming theory [11, 12], banking systems [13, 14], energy [15, 16], Internet of Things (IoT) [17], tracking systems [18]. Among the most significant recent developments is the integration of blockchain with IoT systems. IoT applications have widely adopted blockchain technology due to its extensive feature set, particularly its confidentiality and integrity guarantees. These advantages have motivated researchers to design blockchain-enabled IoT architectures that effectively meet IoT requirements. Existing literature contains numerous proposals and reviews addressing blockchain-IoT integration [19]. Several researches have mentioned how the integration between IoT and blockchain is achieved [20]. Studies have demonstrated that blockchain can secure large-scale data generation while preserving content privacy. This growing research interest has led to widespread

Received October 2025, Received in received from November 2025, Accepted December 2025, and Published December 2025

blockchain adoption across diverse digital information applications and information systems.

Consequently, blockchain technology has demonstrated substantial impact across multiple fields due to its distinctive properties and features. It has effectively addressed various digital information challenges, particularly regarding content quality during processing and transmission. Furthermore, blockchain's decentralized distribution mechanism has resolved issues associated with third-party authentication, significantly improving computation time and transaction processing speed within peer-to-peer networks, where high transaction volumes frequently cause delays.

Blockchain networks occasionally experience structural splits, resulting in two distinct branches: soft forks and hard forks. In soft fork scenarios, network participants can continue operations without upgrading to newer blockchain versions. However, hard forks require all members to adopt updated protocols to maintain network communication and interoperability. Table I summarizes key fields where blockchain technology has been applied, as identified in previous studies.

TABLE I. A LIST OF A NUMBER OF FIELDS RELATED TO THE BLOCKCHAIN TECHNOLOGY

Field of study	Reference
E-Commerce	[8]
Cloud Computing	[9]
Gaming Theory	[10, 11]
Banking Systems	[12, 13]
Energy	[14, 15]
Internet of Things	[16]
Tracking Systems	[17].

III. TYPES OF BLOCKCHAIN-BASED TRACKING AND TRACING SYSTEMS

Westerkamp, Victor, and Küpper [22] developed a blockchain-based method for implementing traceability functions in manufactured products. Traditional tracking solutions often employ fixed digital codes or tokens that are difficult to modify when requirements change. Blockchain-based traceability approaches address this limitation by generating dynamic, easily immutable tokens. The proposed system automatically creates tokens for processed items, enabling comprehensive tracing from initial inputs to finished goods. The ledger was designed to provide visibility into the traceability function, allowing tracking of goods including original inputs. Implementation and evaluation demonstrated successful product tracking across multiple test inputs. The method generates immutable tokens for product tracing. However, the study only covered selected supply chain management phases, which represents a limitation. Potential applications include traceability systems for products during production and distribution.

Hew et al.[23]. investigated blockchain-based product traceability possibilities, aiming to enhance supply chain operations for specific product categories. While blockchain-based tracking systems are widely applicable, certain product types may resist information sharing due to various constraints. The study sought to identify which supply chain products can effectively share tracking and tracing information. An analytical approach collected participant data, employing a mathematical model for analysis. Results revealed that certain product types are unsuitable for blockchain-based tracking systems. The proposed solution enhances product security and demonstrates suitability for supply chain management applications.

Mitani and Otsuka [24] designed a permissioned blockchain-based traceability system to address privacy and security limitations in existing solutions. The research proposes an asset-focused traceability system, incorporating both permissioned and permissionless blockchain architectures. An encryption scheme protects plaintext data. Evaluation results demonstrated that integrating both blockchain types improves tracking and tracing functions regarding security and performance metrics. The system enhances overall tracking security and is applicable to asset traceability systems.

Lin et al. [25] identified product traceability challenges and developed a blockchain-based solution to prevent these issues. Traditional tracking systems often expose recorded and shared data to discovery risks across network nodes. The proposed approach implements a blockchain-based traceability method ensuring product safety during tracking. The system integrates IoT devices to streamline information sharing and employs smart contracts to protect shared data from unauthorized access. Results demonstrated effective data protection, reduced computational costs, decreased data sharing overhead, and decentralized architecture. The system offers cost-effective traceability for tracked products. However, further evaluation is needed regarding usability and computation time for block generation across the tracking network. Applications include traceability systems for medium-scale enterprises.

Hayati and Nugraha [26] investigated blockchain's potential to resolve data integration challenges in tracking and tracing systems without third-party intervention. Blockchain's inherent integration capabilities, eliminating intermediary requirements, form the basis of their approach. The study notes that tracing operations consume substantial computation time, potentially compromising data integrity, and often requiring third-party involvement. Addressing these scenarios would enhance tracking system performance and data privacy. The proposed blockchain-based tracking system implements a

depth-first search algorithm for retrieving data from distributed blockchain networks. Evaluation confirmed successful implementation regarding distribution, verification, and immutability. A key advantage is the dedicated search algorithm for tracking recorded transaction data. However, transaction processing remains slow and complex. Food supply chain and product traceability applications represent potential implementation targets.

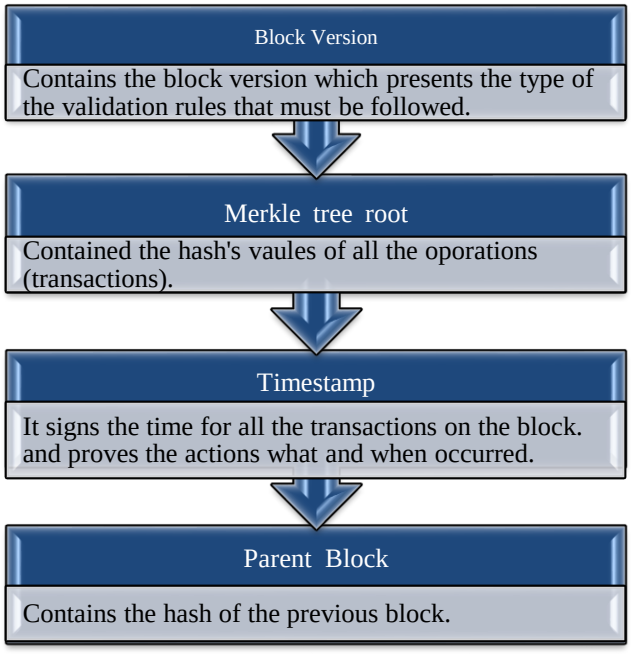
IV. IDENTIFY AND NAME CONCEPT OF BCT

A block can be defined as a collection of transactions recorded in a ledger during a specific time interval. Each blockchain implementation defines unique parameters for block generation, including time periods, size limits, and triggering events. While some blockchains maintain records exclusively for cryptocurrency movements, others manage various types of digital assets. Understanding transactions as data records with assigned values, similar to financial transactions, facilitates comprehension of blockchain's information management capabilities [27].

The chain refers to the cryptographic hash that connects consecutive blocks, creating an unbreakable linkage between them. This concept represents one of blockchain's most sophisticated features, establishing mathematical trust relationships among network participants. The hash function generates a unique fingerprint from each block's data content, establishing both temporal ordering and chronological sequence within the blockchain. This chaining mechanism ensures that any modification to a block becomes immediately detectable throughout the network. The combination of private and public blockchains creates hybrid blockchain architectures that exploit advantages from both types. This enables organizations to maintain both public (permissionless) and private (permission-based) systems simultaneously. Users can rely on hybrid systems to control data access, allowing public visibility for selected information while keeping sensitive data within private networks. Hybrid blockchain systems offer flexibility, enabling users to merge private blockchains with multiple public chains. In hybrid architectures, transaction verification typically occurs within private networks, though transactions can be released to public blockchains for additional verification. Public blockchains require more nodes for verification purposes due to increased hashing requirements, which enhances transparency and overall system security [28].

Blockchain technology organizes information into blocks connected through hash-based chains. Each block consists of two primary components: the Block Header and the Block Body [29]. The Block Header as shown and explained in fig1, contains the block version, Makle tree root, timestamp, and parent block.

TABLE II. ILLUSTRATES THE CONTAINS OF THE HEADER IN EACH BLOCK



While the block body contains on transactions and transition counter, the size of the block and size of the transaction are the measurement that will control the maximum limit of transactions.

V. THE RESEARCH PROBLEM

Blockchain technology has been adopted across numerous application domains, with tracking systems representing a particularly active area of research. Existing literature contains multiple examples of blockchain-based tracking implementations [30] [31] [25]. Salah et al. [32], proposed a blockchain-based system for efficiently managing commercial transactions within supply chain tracking operations.

Various tracking systems employ different technological approaches. Singh et al [33] utilized RFID technology for traceability tasks involving selected elements distributed across different locations within a confined area [34]. Additionally, QR code technology has emerged as an effective tracking solution. QR codes offer superior data storage capacity compared to alternative techniques and provide faster response times. These advantages have enabled QR code integration with IoT systems for real-time tracking applications. Consequently, numerous smart applications, including tracking systems, have adopted QR code technology. Dong et al. provide a detailed example of a QR-based tracking system used to monitor production processes across multiple phases. This approach reportedly reduces computational complexity and processing time efficiently.

VI. IDENTIFY THE TYPES OF THE BCT

A. Public Blockchain

Public or open blockchain technologies provide platforms for interaction between diverse users while protecting transaction parties' identities through anonymity or pseudonymity. In open blockchains, transaction privacy is minimal, as all transactions remain visible to all participants. These systems require substantial computational resources to maintain large-scale distributed ledgers. Consensus achievement in most public blockchains requires each network node to solve complex cryptographic problems called proof-of-work, ensuring all nodes remain synchronized. Prominent examples include Bitcoin, Litecoin, and Ethereum. Ethereum differs from Bitcoin and Litecoin in its processing approach, being primarily utilized for smart contracts—self-executing blockchain code that automatically enforces agreement terms between parties [35]. Common public blockchain implementations include Ethereum, Litecoin, Bitcoin, and most existing cryptocurrencies [36]. Public blockchains are particularly attractive because they require no infrastructure investment, being self-sustaining networks that reduce management costs and overhead [37].

B. Private Blockchain

Private blockchains operate within closed environments where node identities are known. These systems can employ distributed consensus algorithms and smart contracts to efficiently execute complex tasks, surpassing proof-of-work-based blockchains in performance, while also achieving Byzantine fault tolerance [38].

Private or permissioned blockchains are particularly relevant for institutions managing timestamped ledgers or registries, especially in jurisdictions requiring registration of registry processors. These systems provide more predictable and controlled environments compared to permissionless alternatives. Unlike cryptocurrencies, private blockchains do not depend on native tokens for incentivizing transaction processors [39]. ; Instead, processors are rewarded through other mechanisms. Transactions in private blockchains remain confidential, with data inaccessible to the public while member identities are known. Participants cannot read or write to the blockchain without network permission. Common applications include large enterprises where permissions are defined among various stakeholders. For example, banks can maintain private blockchain networks for internal use, restricting access to employees, suppliers, and customers [40].

C. Hybrid Blockchain

Hybrid blockchain represents a subsequent blockchain class developed to combine private and public blockchain advantages, particularly public blockchain scalability and private blockchain block generation rates [41]. Consortium or federated blockchains operate under the control of organizational groups formed around common interests [42]. Various entities including governmental organizations, banks, and private blockchain companies offer different federated blockchain implementations.. Consortium blockchains, like private blockchains, function as permissioned systems allowing only limited participants to perform read and write operations. While all network participants typically can read blockchain data, only trusted few can execute this function. With pre-approved and known participant identities, consortium blockchains achieve faster operation than public blockchains. Additionally, these systems consume less energy by employing voting-based consensus protocols. Federated blockchains can approve transactions in approximately one second [43].

VII. IDENTIFY CONCEPTS RELATED TO THE BLOCKCHAIN

A. The Decentralization

Decentralization refers to a distributed accounting approach where multiple nodes operate across different locations, with each node making its information publicly available for monitoring and supervision. This mechanism aims to enhance transaction legitimacy. All transaction data is recorded in the ledger, with updated information accessible to all participants for monitoring purposes [44] [27].

B. The Ledger

The ledger serves as a comprehensive record of all system activities, accessible to and trusted by all participants. Distributed Ledger Technology (DLT) enables maintenance of a global ledger using append-only data structures across mutually untrusted participants on a distributed platform. Distributed ledgers are characterized by immutability, decentralized maintenance, censorship resistance, and independence from trusted third parties.

C. Peer-to-Peer networks (P2P

Peer-to-Peer (P2P) networking is not a novel concept, as its benefits have been recognized for many years. P2P networks consist of distributed resources interconnected through network infrastructure. Various attempts have been made to comprehensively define P2P networks beyond application-specific descriptions. While P2P can be simply described as the opposite of Client/Server architectures, a more nuanced perspective distinguishes P2P networking based on the "serv-ent" concept—nodes that function simultaneously as both servers and clients. The term "serv-ent" combines the first syllable of "server" with the second syllable of "client." This dual-role capability fundamentally differentiates P2P networks from Client/Server architectures, where nodes serve exclusively as either servers or clients [45].

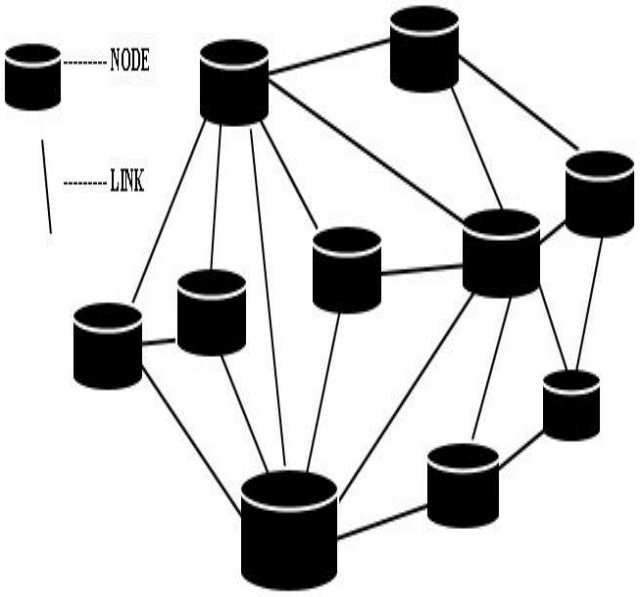


FIGURE 1. Peer-to-Peer networks (P2P)

VIII. Identify surrogate terms and relevant uses of the concept

Blockchain technology has applications across numerous domains. Currently, the most recognized application is distributed ledger technology for digital currencies, commonly known as cryptocurrencies. However, in recent years, private sector organizations and governmental institutions have increasingly adopted blockchain features that align with their operational requirements. Consequently, blockchain adoption has grown substantially across many sectors [46].

A. Distributed systems (DS)

Distributed systems are characterized by two fundamental features. First, they consist of networks of computing elements capable of independent operation. A computing element, referred to as a node, may be either a software process or a hardware device. Second, users typically perceive distributed systems as a single unified system, meaning autonomous nodes must cooperate to achieve this perception. Determining how to establish this cooperation remains the central challenge in distributed systems development. No assumptions are made regarding node types, as distributed systems range from small sensor network devices to high-performance mainframe computers. Similarly, no assumptions exist regarding interconnection methods. Modern distributed systems incorporate diverse node types, from compact plug computers to large-scale high-performance systems. The fundamental principle is that nodes can operate independently, though nodes that ignore each other would serve no purpose in a distributed system. In practical applications, nodes are configured to achieve common goals through message exchange. When a node receives a message, it processes the information and forwards it through message passing mechanisms [47].

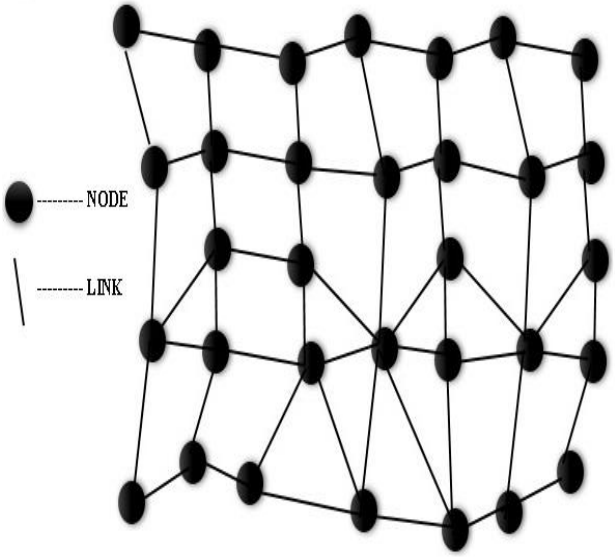


FIGURE 2. Distributed system (DS).

B. Smart Contracts

In 1996, computer scientist Nick Szabo predicted that technological advancement would eventually enable algorithms to manage all forms of contractual arrangements. Despite the brilliance of Szabo's vision, his ideas were considered ahead of the available infrastructure required for implementation [48].

Smart contracts represent a blockchain technology with potential to revolutionize transactions ranging from legal agreements to IoT applications. Smart contracts consist of algorithmic code operating on a peer-to-peer network model. For example, a smart contract can algorithmically implement agreement terms without requiring legal documentation. This enables transaction completion without lawyers or notaries, with transactions being irreversible, trackable, and self-enforcing.

Consider estate administration, where an executor distributes a deceased person's assets [49]. A programmable, legally binding smart contract could serve the same purpose without requiring an executor, using blockchain technology without intermediaries, thereby improving efficiency. The Chainlink network enables smart contracts across existing networks for applications and external data integration, facilitating smart contract payments to designated accounts and creating secure cross-chain connections.

Smart contracts also enable IoT resource and service sharing, creating decentralized service marketplaces between devices and users with cryptographically verifiable automation [50].

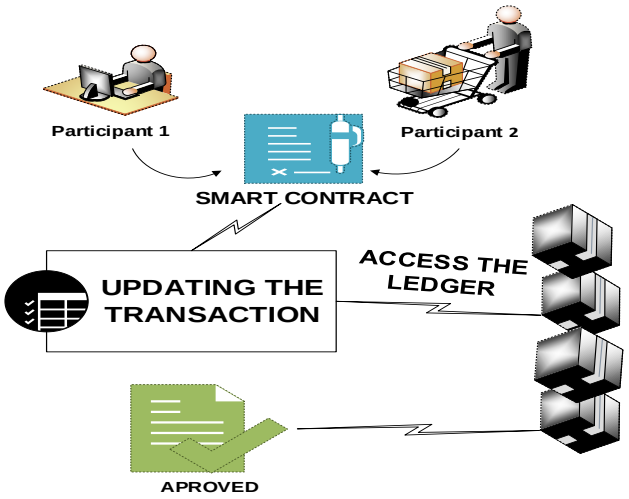


FIGURE 3. Smart contract.

IX. IDENTIFY AND SELECT AN APPROPRIATE REALM (SAMPLE) FOR DATA COLLECTION

A. Cryptocurrency

Cryptocurrency refers to digital currency that utilizes encryption techniques to ensure data and transaction security. It employs decentralized methods to secure payment processing. Cryptocurrency relies on blockchain technology, which maintains a complete record of all transactions conducted by currency holders [51]. Bitcoin was the first cryptocurrency introduced by Satoshi Nakamoto in 2008 and has since become the most widely used cryptocurrency. Following Bitcoin's introduction, over 900 cryptocurrencies have emerged, including altcoin, Ethereum, Ripple, and others [51] [52]. Cryptocurrency functions as a peer-to-peer digital exchange system that depends on cryptography for generating and distributing currency units [53].

B. Internet of Things.

In this system, transactions are verified through distributed networks without central authority oversight. During transaction verification (referred to as mining), critical aspects include transaction amounts, verification that the initiating party possesses the currency being spent, and prevention of double-spending. Various mining technologies are employed based on specific cryptocurrency requirements [54]. For instance, some cryptocurrencies prioritize limiting validated transactions per time unit, while others focus on lightweight and fast service delivery. Certain mining frameworks require substantial memory capacity, whereas others demand significant computational resources. This paper reviews and analyzes cryptocurrency mining techniques with emphasis on their efficiency.

C. Finance Sector

Current electronic payment systems depend on trusted central third parties for secure transaction processing. Efforts to reduce transaction costs have led banks to accept claims on each other, enabling customers to deposit other banks' notes directly without prior conversion to money or gold [58] However, accepting notes from other banks creates settlement delays while arrangements for gold settlement are made.

In scenarios where only limited banks can accept notes, bilateral settlement approaches are employed. As banking systems expand, interbank payments become increasingly complex, with growing incentives for establishing more efficient systems. Financial sector transactions (including global financial and interbank operations) utilize closed distributed ledgers. Given the sector's emphasis on reliability, efficiency, and stability, closed distributed ledger-based blockchains are preferred as they restrict participation to authorized personnel.

Closed ledger systems employ consensus mechanisms that guarantee transaction authenticity by limiting participation to specific groups, eliminating openness-related issues. This approach provides several advantages:

First, it ensures standardization and technological development. Open-type systems struggle with standardization due to technological evolution, while closed-type systems readily accept technical standards among participants

[59]. Second, open ledgers guarantee independence and efficiency. While open-type ledgers avoid external intervention from authorities or regulatory agencies, their efficiency falls below closed-type systems.

Third, closed-type systems permit transaction modifications, whereas open-type systems maintain immutable transaction records (modifications only possible through transaction reversal). Closed-type systems enable modification through mutual agreement. Consequently, closed distributed ledgers are typically adopted in the financial sector.

X. IDENTIFY THE ATTRIBUTES OF THE BCT.

A. The Security of Blockchain

Blockchain security relies on user consensus and mutual trust among participants, establishing a novel security paradigm previously unavailable in network environments. Every network participant maintains a copy of the distributed ledger, providing full visibility of all network activities. When a transaction is initiated, all network nodes observe the action, verify the user's authorization, and must collectively approve the transaction; otherwise, it is rejected. This consensus mechanism delivers high security through distributed verification. To commit fraud, an attacker would need to compromise all network nodes simultaneously—an infeasible proposition given current technological capabilities [60, 61]. Despite blockchain's strong security posture, it faces ongoing threats that may impact its security performance.

B. Transparency and trust

transparency, as all participants can observe network activities. This transparency fosters trust, particularly

important in applications like fund distribution or benefit disbursement where personal discretion restrictions apply.
Consensus represents agreement among distrusting nodes regarding data state. Achieving consensus requires various algorithms. While agreement between two nodes is straightforward, reaching consensus among multiple nodes in distributed systems presents significant challenges. Distributed consensus is therefore defined as the process of achieving agreement across multiple network nodes [62].

C. Fast dealing and cost saving

Blockchain offers faster and more cost-effective operations primarily because it eliminates third-party intermediaries and their associated costs and delays. Financial transactions typically involve multiple intermediaries including banks, custodians, regulators, agents, clearing houses, and government registrars. For example, real estate transactions require involvement from banks, attorneys, notaries, and government entities, each imposing fees or transfer taxes [63]. Blockchain implementation in such transactions significantly reduces time and costs by requiring all parties to maintain data copies, minimizing errors, and eliminating reconciliation requirements.

When financial statements are deemed accurate, auditors receive recognition for their work. However, scandals like the Enron case (2001) eroded public trust in auditors and the overall system. In response, regulations like the Sarbanes-Oxley Act were introduced, increasing organizational compliance costs for forensic auditors, accountants, and IT infrastructure. Blockchain offers a cost-effective alternative for auditing and accounting, as demonstrated by various blockchain designs for distributed financial ledgers [63].
Smart contracts represent automated contract performance, executing only when predetermined conditions are met, eliminating third-party involvement. This cost-effective mechanism provides speed, trust, and efficiency to economic actors, facilitating transactions and payments upon goods delivery [64].

XI. TRACKING AND TRACING SYSTEMS (TTS)

Tracking and tracing systems are designed to determine the location of a unit (such as a device or product) at its current position and at previous positions across different time periods [65]. All location-related information is stored in databases in real-time for subsequent processing. In some implementations, these systems can also store departure and arrival details related to products. The stored information typically includes object identification, transaction timestamps, and location data.
Numerous studies have examined the challenges faced by tracking and tracing systems, along with their features and advantages. For instance, Shamsuzzoha and Helo [66] proposed a system for efficiently managing shipped units and analyzing applied technologies for real-time tracking services. Current tracking and tracing systems encounter various challenges, particularly the management of large data volumes that must be processed efficiently to meet real-time requirements. These difficulties often stem from extensive coordination-related data and details.

XII. BLOCKCHAIN BASED TTS

Traceability represents a key function implemented within tracking and tracing systems that records product-related information throughout movement, shipping, and transitions between locations until the final destination is reached [67]. This tracing capability serves critical purposes including shipping logistics and food safety compliance.
Numerous tracking and tracing systems have adopted blockchain technology. Since its emergence, blockchain has contributed significantly to various application domains by enhancing safety and trustworthiness. This contribution has progressively replaced conventional tracking techniques and other supply chain services, including identification, information processing and sharing, shipping operations, and others. Blockchain implementations have successfully addressed numerous challenges that these systems faced prior to its introduction.

XIII. ISSUES AND HAZARDS OF DATA SIZE EXPLOSION AND GROWTH ON SECURITY AND DECENTRALIZATION OF BLOCKCHAIN

In blockchain networks, exponential data growth has emerged as a significant obstacle to decentralization, which remains a fundamental characteristic of blockchain technology [68]. Figure 4 illustrates this relationship [69]. This represents one of several drawbacks associated with blockchain implementation. Another limitation is that records must remain re-derivable and historical data must be continuously preserved. While this procedure supports security requirements, it simultaneously generates substantial data volumes [70]. Given blockchain's essential nature, maintaining these records is critical. Decentralized entities such as computers face considerable challenges processing these massive datasets. Beyond processing limitations, storage requirements present additional difficulties. When devices lack sufficient storage capacity, the system becomes compelled to process data centrally, potentially undermining blockchain's decentralized architecture.
Multiple studies [68] [71] [72], have identified large blockchain size as a centralization risk. If data continues to explode in terms of size, only a limited number of large enterprises may possess the capability to operate full nodes [73].

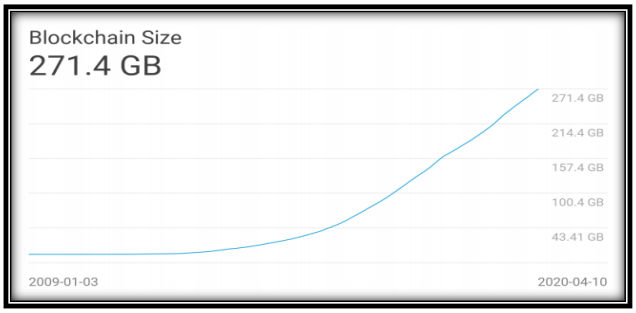


FIGURE 4. **Blockchain size growth as of an exponential relation**

The continuous growth of blockchain data represents a significant hazard. Consider a scenario where data explodes and only a few large corporations can maintain full nodes. This situation raises concerns about potential collusion—these full nodes might unite to manipulate the system for profit, such as altering block rewards. Such manipulation would be difficult for light nodes to detect. However, at least one honest full node would likely share information about the breach, though this sharing could take several hours. Subsequently, light nodes and ordinary users would attempt to blacklist the compromised block. Nevertheless, a coordinated attack on a similar scale to ordinary operational efforts could potentially achieve 51% control. For blockchain-based secure systems containing sensitive information—or in the case of Bitcoin—this represents a serious vulnerability [74].

Analysis of currently published literature indicates that the substantial increase and explosion of blockchain data size poses potential hazards not only to decentralization but also to security, storage capacity, and processing capabilities [75].

XIV. RECENT ANALYTICAL REPORTS

Analytical reports, studies, and research investigations have demonstrated that blockchain data size increases continuously, not only across years but even within months. A recent analytical report published on the Statista website [76] reveals a rapid upward trend in data size growth, with blockchain data expanding from modest sizes to hundreds of gigabytes. The data size is presented with monthly measurements spanning January 2009 to April 2024, as illustrated in Figure 4.

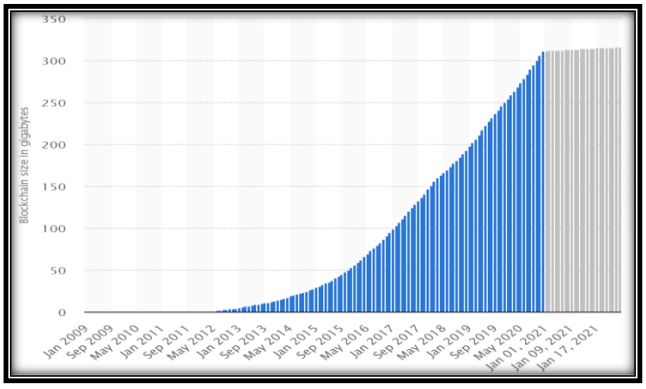


FIGURE 5. **Blockchain data size (in gigabytes) between January 2009 and January 2021.**

As shown in Figure 5, the relationship between the x-axis (months) and y-axis (data size in gigabytes) demonstrates direct proportionality. A critical observation from Figure 2.4 is that data explosion for 2024 is measured in days, with the graph showing an increase from 311.63GB on January 1, 2021 to 550.91GB on April 11, 2024.

Previous studies on data explosion in blockchain applications and services indicate that successful individual-level blockchain adoption will likely increase data size to nearly terabytes. In Figure 6, as of February 1, 2021, data size reached 326.18GB, representing a 10GB increase from its January 1, 2021 level [77].

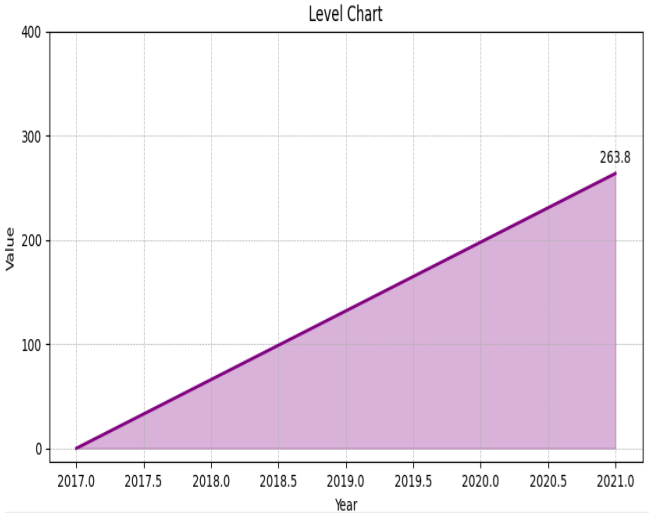


FIGURE 6. **A representation graph of data size explosion in blockchain.**

As of February 22, 2021, the Bitcoin blockchain data size measured 330.24GB, as shown in Figure 2.6 according to[18].

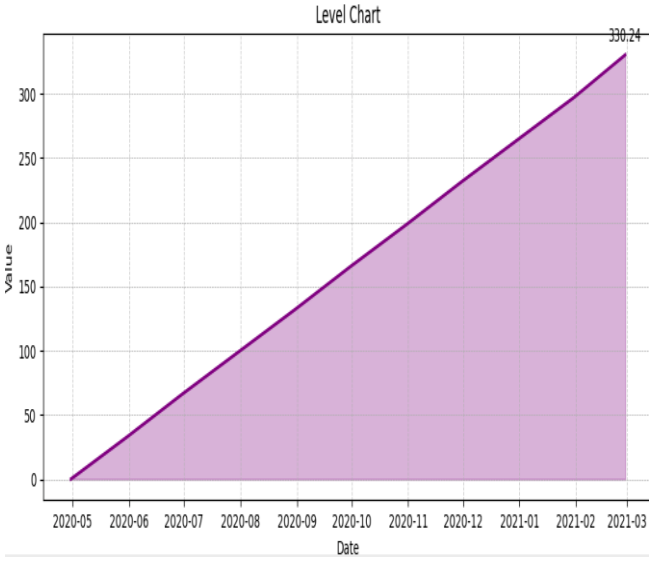


FIGURE 7. **A representation graph of data size explosion in blockchain as of February 22, 2021.**

XV. Analysis related to Data Storage Techniques applied to Data of Blockchain Network

Analysis to give a comprehensive overview about techniques and methods applied to perform data storage mechanisms applied to data of blockchain are summarized in Table III.

TABLE III. LITERATURE REVIEW AND ANALYSIS RELATED TO DATA STORAGE TECHNIQUES APPLIED TO DATA OF BLOCKCHAIN NETWORK

Ref.	Problem statement	Method	Concluded Remarks
[19]	Blockchain size grows exponentially, hindering data-heavy applications.	Blockchain segmentation into multiple segments; each node stores one copy per segment, reducing overall copies stored across nodes.	The method stores one copy per blockchain segment. However, security vulnerabilities arise as data becomes susceptible to loss.
[20]	Health-related data significantly increases blockchain size. Storage space constraints conflict with growing information requirements.	Serial aggregated signature scheme with user/inquirer verification. Privacy protection through verification matching between searched data and requesting user. Signature compression reduces storage requirements.	The method enhances security while potentially reducing blockchain ledger transparency.
[21]	Smart application data storage lacks adequate security. Blockchain integration proposed to enhance data security.	Aggregated signature scheme incorporating proxy verification. Method implements verification protocols and data compression.	This approach can verify blockchain-stored content and data, enabling specific nodes (such as managers) to access user-related information.
[22]	Blockchain faces significant storage size challenges requiring optimization of data storage methods.	Storage mechanism based on algebraic operations utilizing remainders.	Not specified.

XVI. Analysis based on main topic and application of selected past studies

Table IV summarizes numerous research studies across four categories: main topic addressed, potential applications, advantages, and disadvantages of proposed blockchain-based methods or systems.

TABLE IV. ANALYSIS BASED ON MAIN TOPIC AND APPLICATION OF SELECTED PAST STUDIES

Ref.	Main topic & consideration	Potential Application	Advantages	Disadvantages
[23]	Blockchain-related fields	Asset management, government tax payment	Suitable for government tax fee processing	Not specified
[24]	Blockchain-related fields	Asset management, conditional payment	Cost-effective for asset registration management	Lacks access control policies and other smart contract types
[25]	Blockchain-related fields	Secure insurance	Suitable for peer-to-peer insurance applications	Not specified
[26]	Blockchain-related fields	Smart payment systems	Enables payment upon valid verification	Multiple smart contract executions cause interaction overhead
[27]	Blockchain-related fields	Payment systems	Reasonable implementation cost	Not specified
[28]	Blockchain-related fields	Smart property	Suitable for insurance companies and data owners to transact connected car data	Requires processing large data volumes; incompatible with blockchain-based smart contracts
[29]	Blockchain-related fields	Smart appliances	Enables tokenization of smart car services (e.g., car rentals)	Not specified
[30]	Tracking systems	Logistics and supply chain networks	Enables online information processing with appropriate technology	Requires consideration of practical tracking and tracing implementation

Ref.	Main topic & consideration	Potential Application	Advantages	Disadvantages
[31]	Tracking systems	Not specified	Contributes real and representative data	Conventional methods face information sharing challenges
[32]	Tracking systems	Not specified	Utilizes stored product-related data	Traceability limited to specific applications
[33]	Tracking systems	Supply chain management	Enhances tracking and tracing operations during shipping	Requires efficiency evaluation under multi-party data reception conditions
[34]	Tracking and tracing techniques	E-health, e-commerce, cloud-based manufacturing	Low-cost design	Untested efficiency performance
[35]	Tracking and tracing techniques	Item packaging and tracing	Cost-effective solution	Not specified
[36]	Tracking and tracing techniques	Small item packaging and product tracing	Automatic product identification through information extraction	Identification process limited to specific conditions
[37]	Tracking and tracing techniques	Product classification and direction detection	Efficient detection of product movement direction	Suitable only for specific application types
[38]	Blockchain-based tracking	Production traceability applications	Generates immutable tokens for product tracing	Limited to selected supply chain management phases
[39]	Blockchain-based tracking	Supply chain management	Enhances product security	Not specified
[40]	Blockchain-based tracking	Asset traceability systems	Enhanced tracking and tracing system security	Not specified
[41]	Blockchain-based tracking	Small and medium-scale food enterprise traceability	Cost-effective traceability for tracked products	Requires evaluation of usability and block generation computation time
[42]	Blockchain-based tracking	Food supply chain and product traceability	Implements search algorithm for tracking transaction data	Slow transaction implementation with complex processing

XVII. Conclusion

This paper began by examining blockchain technology fundamentals, associated concepts, and its application in tracking and tracing systems. While researchers in the blockchain domain continue to face numerous challenges and difficulties, our investigation specifically focused on the issue of rapidly growing data within blockchain networks. This data growth stems from the substantial number of transactions occurring between nodes and blocks across the network. This concern has gained increasing attention as blockchain adoption expands, with researchers, blockchain platforms, and industry experts actively addressing this dilemma through algorithm design modifications and selective disabling of certain blockchain features.

In our view, blockchain technology has already provided solutions to critical challenges including security, centralization, and real-time transaction processing. However, data explosion within blockchain networks will likely emerge as the foremost priority requiring resolution in future blockchain development efforts.

REFERENCES

[1] M. M. A. Montaser, S. H. Othman, and R. Z. R. M. Radzi, "Secured Tracking and Tracing System Based on Blockchain Technology," in *2021 3rd International Cyber Resilience Conference (CRC)*, 2021: IEEE, pp. 1-6.

[2] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Computers & Security*, vol. 97, p. 101966, 2020/10/01/ 2020, doi: https://doi.org/10.1016/j.cose.2020.101966.

[3] A. Gurtu and J. Johny, "Potential of blockchain technology in supply chain management: a literature review," *International Journal of Physical Distribution & Logistics Management*, vol. 49, no. 9, pp. 881-900, 2019.

[4] H. Wu *et al.*, "Blockchain for finance: A survey," *IET blockchain*, vol. 4, no. 2, pp. 101-123, 2024.

[5] V. Maurya *et al.*, "Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions," *Peer-to-Peer Networking and Applications*, vol. 18, no. 1, p. 53, 2025.

[6] K. Christidis, D. Sikeridis, Y. Wang, and M. Devetsikiotis, "A framework for designing and evaluating realistic blockchain-based local energy markets," *Applied Energy*, vol. 281, p. 115963, 2021/01/01/ 2021, doi: https://doi.org/10.1016/j.apenergy.2020.115963.

[7] M. Muneshwara, T. Shivakumara, M. Swetha, G. Jai Arul Jose, V. V. Kallur, and A. Chethan, "A Blockchain-Internet of Things Solution: Transforming Healthcare Data Security and Efficiency With Enhanced Proof of Stake," in *2026 2nd International Conference on Computing for Sustainability and Intelligent Future (COMP-SIF)*, 2026: IEEE, pp. 1-8.

[8] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A Survey on Blockchain for Information Systems Management and Security," *Information Processing & Management*, vol. 58, no. 1, p. 102397, 2021/01/01/ 2021, doi: https://doi.org/10.1016/j.ipm.2020.102397.

[9] S. Mazumdar, R. J. Kauffman, T. Jensen, R. R. Mukkamala, and J. Damsgaard, "Developing blockchain-based transparent e-commerce solutions for Danish SMEs to promote sustainable design products," *Blockchain: Research and Applications*, vol. 7, no. 2, p. 100330, 2026.

[10] K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain Meets Cloud Computing: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2009-2030, 2020.

[11] Z. Liu *et al.*, "A survey on applications of game theory in blockchain," *arXiv preprint arXiv:1902.10865*, 2019.

[12] M. H. Manshaei, M. Jadliwala, A. Maiti, and M. Fooladgar, "A Game-Theoretic Analysis of Shard-Based Permissionless Blockchains," *IEEE Access*, vol. 6, pp. 78100-78112, 2018.

[13] N. A. Popova and N. G. Butakova, "Research of a Possibility of Using Blockchain Technology without Tokens to Protect Banking Transactions," in *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, 28-31 Jan. 2019 2019, pp. 1764-1768.

[14] N. R. Bagrecha, I. M. Polishwala, P. A. Mehrotra, R. Sharma, and B. S. Thakare, "Decentralised Blockchain Technology: Application in Banking Sector," in *2020 International Conference for Emerging Technology (INCET)*, 5-7 June 2020 2020, pp. 1-5.

[15] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K. K. R. Choo, "An Energy-Efficient SDN Controller Architecture for IoT Networks With Blockchain-Based Security," *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 625-638, 2020.

[16] A. Sheikh, V. Kamuni, A. Urooj, S. Wagh, N. Singh, and D. Patel, "Secured Energy Trading Using Byzantine-Based Blockchain Consensus," *IEEE Access*, vol. 8, pp. 8554-8571, 2020.

[17] N. K. Tran, M. Ali Babar, and J. Boan, "Integrating blockchain and Internet of Things systems: A systematic review on objectives and designs," *Journal of Network and Computer Applications*, vol. 173, p. 102844, 2021/01/01/ 2021, doi: https://doi.org/10.1016/j.jnca.2020.102844.

[18] A. Chauhan, G. Savner, P. Venkatesh, V. Patil, and W. Wu, "A Blockchain-Based Tracking System," in *2020 IEEE International Conference on Service Oriented Systems Engineering (SOSE)*, 3-6 Aug. 2020 2020, pp. 111-115.

[19] X. Sun *et al.*, "Reliability techniques and architectures for blockchain-enabled internet of things: Current applications, systematic review, and future trends," *Computer Standards & Interfaces*, p. 104068, 2025.

[20] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," *Journal of Network and Computer Applications*, vol. 125, pp. 251-279, 2019/01/01/ 2019, doi: https://doi.org/10.1016/j.jnca.2018.10.019.

[21] H. Taherdoost and M. Madanchian, "Blockchain-based e-commerce: A review on applications and challenges," *Electronics*, vol. 12, no. 8, p. 1889, 2023.

[22] M. Westerkamp, F. Victor, and A. Küpper, "Tracing manufacturing processes using blockchain-based token compositions," *Digital Communications and Networks*, vol. 6, no. 2, pp. 167-176, 2020/05/01/ 2020, doi: https://doi.org/10.1016/j.dcan.2019.01.007.

[23] J.-J. Hew, L.-W. Wong, W.-H. Tan Garry, K.-B. Ooi, and B. Lin, "The blockchain-based Halal traceability systems: a hype or reality?," *Supply Chain Management: An International Journal*, vol. 25, no. 6, pp. 863-879, 2020, doi: 10.1108/SCM-01-2020-0044.

[24] T. Mitani and A. Otsuka, "Traceability in Permissioned Blockchain," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 14-17 July 2019 2019, pp. 286-293, doi: 10.1109/Blockchain.2019.00045.

[25] Q. Lin, H. Wang, X. Pei, and J. Wang, "Food Safety Traceability System Based on Blockchain and EPCIS," *IEEE Access*, vol. 7, pp. 20698-20707, 2019, doi: 10.1109/ACCESS.2019.2897792.

[26] H. Hayati and I. G. B. B. Nugraha, "Blockchain Based Traceability System in Food Supply Chain," in *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 21-22 Nov. 2018 2018, pp. 120-125, doi: 10.1109/ISRITI.2018.8864477.

[27] M. Swan, *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[28] D. R. Ferrin, "Method and apparatus for the limitation of the mining of blocks on a block chain," ed: Google Patents, 2018.

[29] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," presented at the 2017 IEEE International Congress on Big Data (BigData Congress), 2017.

[30] X. Zhang *et al.*, "Blockchain-Based Safety Management System for the Grain Supply Chain," *IEEE Access*, vol. 8, pp. 36398-36410, 2020.

[31] S. Mondal, K. P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal, "Blockchain Inspired RFID-Based Information Architecture for Food Supply Chain," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5803-5813, 2019.

[32] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchain-Based Soybean Traceability in Agricultural Supply Chain," *IEEE Access*, vol. 7, pp. 73295-73305, 2019.

[33] K. Singh *et al.*, "Localization of Life Safety Vests in an Aircraft Using Backscattering RFID Communication," *IEEE Journal of Radio Frequency Identification*, vol. 4, no. 3, pp. 234-245, 2020.

[34] P. Fathi, N. C. Karmakar, M. Bhattacharya, and S. Bhattacharya, "Potential Chipless RFID Sensors for Food Packaging Applications: A Review," *IEEE Sensors Journal*, vol. 20, no. 17, pp. 9618-9636, 2020.

[35] V. J. Morkunas, J. Paschen, and E. Boon, "How blockchain technologies impact your business model," *Business Horizons*, vol. 62, no. 3, pp. 295-306, 2019.

[36] M. Haferkorn and J. M. Q. Diaz, "Seasonality and interconnectivity within cryptocurrencies-an analysis on the basis of bitcoin, litecoin and namecoin," in *International Workshop on Enterprise Applications and Services in the Finance Industry*, 2014: Springer, pp. 106-120.

[37] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55-81, 2019, doi: 10.1016/j.tele.2018.11.006.

[38] Y. Hao, Y. Li, X. Dong, L. Fang, and P. Chen, "Performance analysis of consensus algorithm in private blockchain," in *2018 IEEE Intelligent Vehicles Symposium (IV)*, 2018: IEEE, pp. 280-285.

[39] T. Swanson, "Watermarked tokens and pseudonymity on public blockchains," *Unpublished manuscript, R3CEV*, 2015.

[40] T. Kitsantas, A. Vazakidis, and E. Chytis, *A Review of Blockchain Technology and Its Applications in the Business Environment*. 2019.

[41] D. S. Rajput, R. S. Thakur, and S. M. Basha, *Transforming Businesses With Bitcoin Mining and Blockchain Applications*. IGI Global, 2019.

[42] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE transactions on industrial informatics*, vol. 14, no. 8, pp. 3690-3700, 2017.

[43] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127-10149, 2019.

[44] J. Y. Lee, "A decentralized token economy: How blockchain and cryptocurrency can revolutionize business," *Business Horizons*, vol. 62, no. 6, pp. 773-784, 2019/11/01/ 2019, doi: https://doi.org/10.1016/j.bushor.2019.08.003.

[45] R. Schollmeier, "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications," in *Proceedings First International Conference*

on Peer-to-Peer Computing, 27-29 Aug. 2001 2001, pp. 101-102, doi: 10.1109/P2P.2001.990434.

[46] S. Liu and S. He, "Application of Block Chaining Technology in Finance and Accounting Field," in *2019 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)*, 12-13 Jan. 2019 2019, pp. 342-344, doi: 10.1109/ICITBS.2019.00090.

[47] M. van Steen and A. S. Tanenbaum, "A brief introduction to distributed systems," *Computing*, vol. 98, no. 10, pp. 967-1009, 2016/10/01 2016, doi: 10.1007/s00607-016-0508-7.

[48] P. Catchlove, "Smart contracts: a new era of contract use," *Available at SSRN 3090226*, 2017.

[49] S. Vujičić, N. Hasanspahić, M. Car, and L. Čampara, "Distributed Ledger Technology as a Tool for Environmental Sustainability in the Shipping Industry," *Journal of Marine Science and Engineering*, vol. 8, no. 5, p. 366, 2020.

[50] S. Makridakis and K. Christodoulou, "Blockchain: Current Challenges and Future Prospects/Applications," *Future Internet*, vol. 11, no. 12, p. 258, 2019.

[51] V. Chauhan and G. Arora, "A review paper on cryptocurrency & portfolio management," in *2019 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC)*, 18-19 Oct. 2019 2019, pp. 60-62, doi: 10.1109/PEEIC47157.2019.8976592.

[52] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2015: Springer, pp. 281-310.

[53] R. Raju, M. SaiVignesh, and K. I. A. Prasad, "A Study of Current Cryptocurrency Systems," in *2018 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC)*, 28-29 March 2018 2018, pp. 203-209.

[54] R. Farell, "An analysis of the cryptocurrency industry," 2015.

[55] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395-411, 2018.

[56] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *Ieee Access*, vol. 4, pp. 2292-2303, 2016.

[57] K. Shehzad, M. Afrasayab, M. Khan, M. A. Mushtaq, R. L. Ahmed, and M. M. Saleemi, "Use of Blockchain in Internet of things: A Systematic Literature Review," in *2019 Cybersecurity and Cyberforensics Conference (CCC)*, 8-9 May 2019 2019, pp. 165-171.

[58] S. Yoo, "Blockchain based financial case analysis and its implications," *Asia Pacific Journal of Innovation and Entrepreneurship*, vol. 11, no. 3, pp. 312-321, 2017, doi: 10.1108/APJIE-12-2017-036.

[59] R. Lewis, J. McPartland, and R. Ranjan, "Blockchain and financial market innovation," *Economic Perspectives*, vol. 41, no. 7, pp. 1-17, 2017.

[60] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, and M. Imran, "Securing IoTs in distributed blockchain: Analysis, requirements and open issues," *Future Generation Computer Systems*, vol. 100, pp. 325-343, 2019.

[61] R. Stephen and A. Alex, "A Review on BlockChain Security," *IOP Conference Series: Materials Science and Engineering*, vol. 396, p. 012030, 2018/08/29 2018, doi: 10.1088/1757-899x/396/1/012030.

[62] J. Biggs, S. R. Hinish, M. A. Natale, and M. Patronick, "Blockchain: Revolutionizing the global supply chain by building trust and transparency," *New Jersey: Rutgers University*, 2017.

[63] D. Brandon, "The blockchain: The future of business information systems," *International Journal of the Academic Business World*, vol. 10, no. 2, pp. 33-40, 2016.

[64] B. Kewell, R. Adams, and G. Parry, "Blockchain for good?," *Strategic Change*, vol. 26, no. 5, pp. 429-437, 2017, doi: 10.1002/jsc.2143.

[65] X. Liu, A. V. Barenji, Z. Li, B. Montreuil, and G. Q. Huang, "Blockchain-based smart tracking and tracing platform for drug supply chain," *Computers & Industrial Engineering*, vol. 161, p. 107669, 2021.

[66] A. Shamsuzzoha and P. T. Helo, "Real-time tracking and tracing system: Potentials for the logistics network," in *Proceedings of the 2011 international conference on industrial engineering and operations management*, 2011, pp. 22-24.

[67] V. Hassija, V. Chamola, V. Gupta, S. Jain, and N. Guizani, "A survey on supply chain security: Application areas, security threats, and solution architectures," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6222-6246, 2020.

[68] Y. Xu and Y. Huang, "Segment Blockchain: A Size Reduced Storage Mechanism for Blockchain," *IEEE Access*, vol. 8, pp. 17434-17441, 2020, doi: 10.1109/ACCESS.2020.2966464.

[69] A. Hafid, A. S. Hafid, and M. Samih, "Scaling Blockchains: A Comprehensive Survey," *IEEE Access*, vol. 8, pp. 125244-125262, 2020, doi: 10.1109/ACCESS.2020.3007251.

[70] Q. Lu, X. Xu, Y. Liu, I. Weber, L. Zhu, and W. Zhang, "uBaaS: A unified blockchain as a service platform," *Future Generation Computer Systems*, vol. 101, pp. 564-575, 2019/12/01/ 2019, doi: https://doi.org/10.1016/j.future.2019.05.051.

[71] D. Gruber, W. Li, and G. Karame, "Unifying lightweight blockchain client implementations," in *Proc. NDSS Workshop Decentralized IoT Security Stand.*, 2018, pp. 1-7.

[72] V. Buterin, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, 2014.

[73] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A Lightweight Scalable Blockchain for IoT security and anonymity," *Journal of Parallel and Distributed Computing*, vol. 134, pp. 180-197, 2019.

[74] M. Zamani, M. Movahedi, and M. Raykova, "RapidChain: Scaling Blockchain via Full Sharding," presented at the Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada, 2018. [Online]. Available: https://doi.org/10.1145/3243734.3243853.

[75] X. Wang *et al.*, "Survey on blockchain for Internet of Things," *Computer Communications*, vol. 136, pp. 10-29, 2019/02/01/ 2019, doi: https://doi.org/10.1016/j.comcom.2019.01.006.

[76] Statista. "Size of the Bitcoin blockchain from January 2009 to January 2021 (in gigabytes)." https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/ (accessed 2 February, 2021).

[77] Ycharts. "Bitcoin Blockchain Size: 330.79 GB for Feb 25 2021." https://ycharts.com/indicators/bitcoin_blockchain_size (accessed 25 February, 2021).

[78] Y. Ren, Y. Leng, F. Zhu, J. Wang, and H.-J. Kim, "Data Storage Mechanism Based on Blockchain with Privacy Protection in Wireless Body Area Network," *Sensors*, vol. 19, no. 10, p. 2395, 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/10/2395.

[79] Y. Ren *et al.*, "Multiple cloud storage mechanism based on blockchain in smart homes," *Future Generation Computer Systems*, vol. 115, pp. 304-313, 2021/02/01/ 2021, doi: https://doi.org/10.1016/j.future.2020.09.019.

[80] H. Mei, Z. Gao, Z. Guo, M. Zhao, and J. Yang, "Storage Mechanism Optimization in Blockchain System Based on Residual Number System," *IEEE Access*, vol. 7, pp. 114539-114546, 2019, doi: 10.1109/ACCESS.2019.2934092.

[81] V. Zakhary, M. J. Amiri, S. Maiyya, D. Agrawal, and A. E. Abbadi, "Towards global asset management in blockchain systems," *arXiv preprint arXiv:1905.09359*, 2019.

[82] Q. Lu *et al.*, "Integrated Model-Driven Engineering of Blockchain Applications for Business Processes and Asset Management," *arXiv preprint arXiv:2005.12685*, 2020.

[83] P. Tasca, "Insurance Under the Blockchain Paradigm," in *Business Transformation through Blockchain: Volume I*, H. Treiblmaier and R. Beck Eds. Cham: Springer International Publishing, 2019, pp. 273-285.

[84] H. Wang, H. Qin, M. Zhao, X. Wei, H. Shen, and W. Susilo, "Blockchain-based fair payment smart contract for public cloud storage auditing," *Information Sciences*, vol. 519, pp. 348-362, 2020/05/01/ 2020, doi: https://doi.org/10.1016/j.ins.2020.01.051.

[85] T. A. Alghamdi, I. Ali, N. Javaid, and M. Shafiq, "Secure Service Provisioning Scheme for Lightweight IoT Devices With a Fair Payment System and an Incentive Mechanism Based on Blockchain," *IEEE Access*, vol. 8, pp. 1048-1061, 2020, doi: 10.1109/ACCESS.2019.2961612.

[86] B.-G. Jeong, T.-Y. Youn, N.-S. Jho, and S. U. Shin, "Blockchain-Based Data Sharing and Trading Model for the Connected Car," *Sensors*, vol. 20, no. 11, p. 3141, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/11/3141.

[87] V. Valaštín, K. Košt'ál, R. Bencel, and I. Kotuliak, "Blockchain Based Car-Sharing Platform," in *2019 International Symposium ELMAR*, 23-25 Sept. 2019 2019, pp. 5-8, doi: 10.1109/ELMAR.2019.8918650.

[88] M. R. Høyer, O. E. Oluyisola, J. O. Strandhagen, and M. G. Semini, "Exploring the challenges with applying tracking and tracing technology in the dairy industry," *IFAC-PapersOnLine*, vol. 52, no. 13, pp. 1727-1732, 2019/01/01/ 2019, doi: https://doi.org/10.1016/j.ifacol.2019.11.450.

[89] J. Wessel, A. Turetskyy, O. Wojahn, C. Herrmann, and S. Thiede, "Tracking and Tracing for Data Mining Application in the Lithium-ion Battery Production," *Procedia CIRP*, vol. 93, pp. 162-167, 2020/01/01/ 2020, doi: https://doi.org/10.1016/j.procir.2020.03.071.

[90] M. A. M'hand, A. Boulmakoul, H. Badir, and A. Lbath, "A scalable real-time tracking and monitoring architecture for logistics and transport in RoRo terminals," *Procedia Computer Science*, vol. 151, pp. 218-225, 2019/01/01/ 2019, doi: https://doi.org/10.1016/j.procs.2019.04.032.

[91] R. Addo-Tenkorang, N. Gwangwava, E. N. Ogunmuyiwa, and A. U. Ude, "Advanced Animal Track-&-Trace Supply-Chain Conceptual Framework: An Internet of Things Approach," *Procedia Manufacturing*, vol. 30, pp. 56-63, 2019/01/01/ 2019, doi: https://doi.org/10.1016/j.promfg.2019.02.009.

[92] B. Fan *et al.*, "Improving continuous traceability of food stuff by using barcode-RFID bidirectional transformation equipment: Two field experiments," *Food Control*, vol. 98, pp. 449-456, 2019/04/01/ 2019, doi: https://doi.org/10.1016/j.foodcont.2018.12.002.

[93] K. Liang *et al.*, "Development and parameter optimization of automatic separation and identification equipment for grain tracing systems based on grain tracers with QR codes," *Computers and Electronics in Agriculture*, vol. 162, pp. 709-718, 2019/07/01/ 2019, doi: https://doi.org/10.1016/j.compag.2019.04.039.

[94] G. Alfian *et al.*, "Improving efficiency of RFID-based traceability system for perishable food by utilizing IoT sensors and machine learning model," *Food Control*, vol. 110, p. 107016, 2020/04/01/ 2020, doi: https://doi.org/10.1016/j.foodcont.2019.107016.