International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An In-Depth Comparative Review of Blockchain Models for Enhancing Traceability in Real-Time Deployments

Mrs. Hemlata Kosare[1], Dr. Amol Zade[2]

Submitted: 16/05/2024 **Revised**: 27/06/2024 **Accepted**: 07/07/2024

Abstract: The necessity for a comprehensive comparative review of blockchain models, especially in the context of enhancing traceability in real-time deployments, is paramount in today's rapidly evolving digital landscape. This paper embarks on this essential exploration, addressing a notable gap in the existing literature: the lack of an in-depth, comparative analysis specifically tailored to real-time blockchain applications with a focus on traceability. Previous reviews in this domain have often been limited by their scope, either concentrating on a narrow aspect of blockchain technology or overlooking the critical component of traceability in real-world implementations for different scenarios. Our review process diverges from these limitations, employing a meticulous and multifaceted approach. We dissect various blockchain models, evaluating them not only for their architectural integrity and efficiency but also for their capacity to facilitate traceability in dynamic environments. This in-depth analysis is further enriched by a comparative methodology, where models are juxtaposed against each other, revealing their respective strengths and shortcomings in practical scenarios. One of the distinguishing advantages of this review lies in its holistic approach. By integrating insights from a diverse range of sources and perspectives, we provide a nuanced understanding of how different blockchain models can be optimized for traceability characteristics. This approach enables us to present a balanced view, acknowledging the complexities and trade-offs inherent in each of the models in different scenarios. The impacts of this review are multifaceted. Firstly, it is a critical source for experts and researchers in the field of blockchain technology, offering a comprehensive guide to selecting and implementing the most suitable models for their specific needs. Secondly, the insights garnered from this comparative analysis have the potential to spur innovation in blockchain development, particularly in enhancing traceability features for real-world applications. Lastly, by addressing the limitations of previous reviews and presenting a more rounded perspective, this paper contributes significantly to the academic discourse, setting a new benchmark for future research in this area for different scenarios.

Keywords: *Blockchain Models, Real-Time Deployments, Traceability, Comparative Analysis, Technological Innovation, Scenarios*

1. Introduction

In the expanding realm of digital technology, blockchain has emerged as a transformative force, heralding a new era of decentralized and secure data management process. The unique attributes of blockchain, characterized by immutability, transparency, and distributed ledger technology, make it an ideal candidate for a myriad of applications, spanning from financial transactions to supply chain management. However, the deployment of blockchain models in real-time environments, particularly with an emphasis on traceability, presents a complex landscape that merits thorough exploration. This paper seeks to delve into this intricate domain, providing an in-depth comparative review of various blockchain models to discern their effectiveness in enhancing traceability within real-time deployments.

The introduction of blockchain technology has revolutionized the way data is stored and transferred, offering unprecedented levels of security and decentralization. Its potential to ensure traceability, a critical aspect in numerous sectors including healthcare, finance, and logistics, is particularly noteworthy. Traceability within these sectors is paramount, as it ensures transparency, accountability, and efficiency. Despite the increasing interest and implementation of blockchain technology, a detailed understanding of its deployment, especially in real-time scenarios where the demand for immediate data processing and verification is high, remains relatively uncharted in real-time use cases. This gap in knowledge and understanding underscores the need for a comprehensive review that not only evaluates different blockchain models but also their specific applicability and efficacy in real-time environments with a focus on traceability characteristics.

Existing literature on blockchain technology often centers on its theoretical aspects or its application in specific case studies. However, there is a paucity of research that systematically compares various blockchain models, particularly in the context of their real-time deployment capabilities and traceability features. This paper addresses this gap by providing a comparative analysis of different blockchain models. It scrutinizes their architecture,

(1) Ph.D. Scholar, Department of Computer Science & Engineering, GHRU Amravati
(2) Assistant Professor, Department of Computer Science & Engineering, GHRU Amravati

performance, scalability, and, most crucially, their ability to enable and enhance traceability in real-time applications.

The introduction of blockchain in real-time systems poses unique challenges. These include handling high transaction volumes, maintaining data integrity in a rapidly changing environment, and ensuring that traceability is not compromised in the process. Furthermore, the suitability of a blockchain model for a particular application is contingent upon various factors such as the characteristics of the data, the required transaction speed, and the degree of decentralization needed. This paper systematically dissects these factors, offering insights into how different blockchain models can be tailored to meet the specific requirements of real-time deployments while maximizing traceability.

In conclusion, the Introduction section of this paper sets the stage for a nuanced and comprehensive examination of blockchain models in the context of real-time deployments with an emphasis on traceability. It highlights the significance of this study in the broader landscape of blockchain technology and emphasizes the significance of a detailed comparative analysis to guide practitioners and researchers in the field. The subsequent sections of the paper will delve into the methodologies employed for this comparative analysis, the findings from this study, and their implications for the future of blockchain technology in real-time applications.

Motivation of this work

The Motivation & Contribution section of this scholarly paper unfolds against the backdrop of an increasingly digitalized world, where blockchain technology has become a cornerstone in various sectors, promising enhanced security, transparency, and efficiency. The motivation for this comprehensive review stems from the critical need to understand and harness the full potential of blockchain models, particularly in enhancing traceability within real-time deployments. This need is driven by the escalating demand for transparent and secure data management in numerous fields, ranging from finance and healthcare to supply chain logistics. In these sectors, the ability to trace transactions or data in real-time is not just a convenience but a necessity, ensuring integrity, compliance, and consumer trust.

The contribution of this paper is multifaceted and significant. Firstly, it provides a comprehensive and comparative analysis of various blockchain models, a study that is conspicuously absent in current academic discourse. This analysis is not merely theoretical but deeply grounded in practical applicability, focusing on real-time deployments and their unique demands. By evaluating different blockchain architectures, the paper sheds light on how each model fares in terms of facilitating traceability, managing transaction loads, and maintaining data integrity in dynamic environments.

Secondly, the paper contributes to the field by offering practical insights for practitioners. The comparative review serves as a guide for professionals in selecting the most appropriate blockchain model tailored to their specific needs, particularly emphasizing the aspect of traceability in real-time operations. This guidance is invaluable in a landscape where technological choices can significantly impact operational efficiency and compliance with regulatory standards.

Moreover, the paper enriches academic research by identifying and addressing gaps in existing literature. It moves beyond the general discussions of blockchain technology to focus on the nuanced differences between various models and their implications for traceability in real-time contexts. This detailed analysis contributes to a deeper comprehension of blockchain technologies, challenging and extending existing theories and models.

Lastly, the paper's contribution extends to the realm of innovation and future research. By highlighting the benefits and drawbacks of various blockchain models in the context of real-time traceability, it opens new avenues for technological advancement. Researchers and developers can draw upon the insights provided to enhance existing blockchain architectures or to innovate new models that better address the complexities of real-time data management and traceability. This aspect of the paper is particularly crucial in an era where technology is rapidly evolving, and adaptability to emerging challenges is key to sustaining progress.

In essence, the Motivation & Contribution section encapsulates the urgency and relevance of this comparative review in the current technological landscape. It articulates the necessity for a deeper, more nuanced understanding of blockchain technologies in real-time applications, especially concerning traceability. This paper fills a critical gap in existing literature and serves as a catalyst for further research and development in this field, aiming to enhance the efficacy, efficiency, and reliability of blockchain deployments in real-world scenarios. The insights and conclusions drawn from this study promise to have a lasting impact on the academic and practical applications of blockchain technology, guiding future innovations and implementations for different scenarios.

2. Brief review of Existing Methods

This, we examine existing scholarly work in the field of blockchain technology, with a particular focus on its application for enhancing traceability in real-time deployments. This review synthesizes a wide range of research, providing cohesive knowledge about the situation of blockchain technology today and its diverse implementations for different scenarios.

Initially, the review delves into foundational studies on blockchain technology. These foundational works, such as Nakamoto's seminal paper on Bitcoin, lay the groundwork for understanding the basic principles of blockchain's decentralized nature, immutability, and the use of consensus algorithms. Building upon these core concepts, subsequent research has explored various blockchain models like public, private, and consortium blockchains, each presenting unique characteristics suitable for different applications.

A significant portion of the review is dedicated to studies focusing on the use of blockchain for traceability. This includes research on supply chain management, where blockchain's ability to provide transparent and immutable records has been leveraged to track the provenance and movement of goods. Key studies in this area demonstrate how blockchain technology can mitigate issues like fraud, counterfeiting, and lack of accountability in supply chains.

Further, the review addresses the challenges and solutions proposed for implementing blockchain in real-time systems. Real-time blockchain deployments, as discussed in various studies, face issues such as scalability, latency, and the handling of large transaction volumes. The literature reveals a range of approaches to tackle these challenges, including innovations in consensus mechanisms, off-chain transactions, and how blockchain is incorporated into scenarios including other cutting-edge innovations in artificial intelligence (AI) and the Internet of Things (IoT).

Additionally, the review covers critical analyses and comparisons of different blockchain models in the context of real-time traceability. It highlights the strengths and limitations of each model, drawing on case studies and practical implementations for different use cases. This comparative analysis is vital in understanding how specific characteristics of blockchain models align with the requirements of various real-time applications.

The literature also explores the regulatory and ethical considerations surrounding blockchain technology. Studies in this domain address the legal implications of blockchain deployments, particularly in terms of data privacy, security, and compliance with international standards. This aspect is crucial in the context of traceability, where sensitive data often needs to be managed in a transparent yet secure manner for different use cases. In synthesizing these diverse strands of research, the Literature Review section not only provides a thorough understanding of the current state of blockchain technology but also highlights the gaps and areas needing further investigation. One such gap is the in-depth comparative analysis of blockchain models for traceability in real-time deployments, which this paper aims to address.

This comprehensive review of existing literature thus sets the stage for the paper's contribution to the field for different use cases. It underscores the need for a nuanced understanding of how different blockchain models can be optimized for real-time applications, particularly in enhancing traceability levels. The insights gleaned from this review are instrumental in guiding the subsequent sections of the paper, where a detailed comparative analysis of various blockchain models is presented, elucidating their potential and limitations in real-time traceability applications.

3. In-depth review of existing methods used for blockchain tracing & security analysis

A wide variety of models are proposed by researchers for analyzing & enhancing traceability of blockchains. The reviewed literature reveals a diverse landscape of research efforts in the field of blockchain traceability and its applications across various domains. These studies collectively underscore the multifaceted nature of blockchain technology and its capacity to address complex issues while introducing innovative solutions. This summary provides a comprehensive overview of the key findings and contributions from the literature.

The first study, discussed in [1], delves into the realm of supply chain traceability, emphasizing the significance of transparency, authenticity, and efficiency. Notably, it addresses the understudied issue of efficiency in blockchain-based supply chain traceability. The research introduces a novel approach involving the replication of records in multiple chunks and parallel search techniques, ultimately yielding a remarkable reduction in time overheads. In [2], the focus shifts towards protecting original achievements and intellectual property rights. The paper presents a blockchain service architecture designed to boost information traceability and safety effectiveness. The future system leverages blockchain's essential features like distributed data storage and encoding techniques, to protect and trail original achievements' recordings and related dealings. The study also introduces an automatic system of rewards and incentives to encourage the production and preservation of unique works of art.

Moving on to [3], the concept of redactable blockchain emerges as a solution to mitigate the misuse of blockchain storage. The research tackles the challenge of dealing with potentially malicious modifiers in existing schemes. It introduces An effective dynamic redactable blockchain that is based on trust that supports updates and traceability. This innovative approach includes the development of a dynamic trust evaluation model, which assesses user reliability comprehensively, and the implementation of a dynamic trust-based chameleon hash to ensure full-process security levels. In [4], the discussion centers on the agriculture supply chain and the importance of product traceability for food safety and customer trust levels. The study introduces a blockchain system with user identification methods, filling a notable gap in existing blockchain traceability systems. Additionally, the research presents a novel Proof of Transaction (PoTx) consensus algorithm designed for scalability and fault-tolerance sets.

Reference Number	**Method Name**	**Findings**	**Advantages**	**Limitations**	**Impacts**
[1]	Blockchain-based Supply Chain Traceability	Improved time efficiency through parallel search and record replication.	Enhances time efficiency in supply chain traceability.	Challenges in record allocation for parallelization.	Positive impact on supply chain transparency and authenticity.
[2]	Blockchain Service for Information Traceability	Utilizes blockchain for information traceability and protection.	Ensures information traceability and protection.	Requires further investigation in different contexts.	Potential for broader blockchain applications in various domains.
[3]	Dynamic Trust-based Redactable Blockchain	Introduces redactable blockchain with dynamic trust that facilitates updating and tracing.	Provides complete process security together with pre-evaluation before modification.	Malicious modifiers may pose challenges.	Improved security and traceability in redactable blockchains.
[4]	Blockchain Traceability in Agriculture Supply Chain	Presents a blockchain system with user identification and Proof of Transaction (PoTx) consensus algorithm.	Enhances traceability and identifies product adulteration.	Lack of focus on user identification in previous work.	Increased trust and transparency in agriculture supply chain.
[5]	Traceability of Onsite Construction Activities	Combines computer vision and blockchain for onsite construction traceability.	Provides high-resolution traceability of onsite construction activities.	Requires integration of cutting-edge deep learning algorithms.	Improves construction process quality and transparency.
[6]	Traceable Self-randomization Certificate Authentication	Introduces a PKI architecture traceable self-randomization certificate authentication system.	Balances user anonymity and traceability in PKI.	Existing PKI architecture lacks privacy protection.	Enhances privacy and traceability in PKI for network communication.
[7]	An NFT-based Approach to the Management of Refurbished Medical Equipment	Proposes an NFT-based solution for medical device management that is reconditioned.	Ensures the safety and quality of refurbished medical devices.	Challenges in the integration of NFTs and tracking.	Increases trust and safety in the use of refurbished medical devices.
[8]	Trackable Anonymous	Presents a trackable,	Protects privacy while enabling	Existing schemes have limitations in	Improves privacy and traceability in

	Remote Healthcare Data Sharing	anonymous system for sharing and storing remote medical data via a decentralized consortium blockchain.	traceability in healthcare data sharing.	privacy and traceability.	remote healthcare data sharing.
[9]	Storage-efficient Vaccine Safety Protection	Proposes an improved, a blockchain-driven, effective vaccination safety protection program for storage.	Addresses large on-chain storage consumption and low throughput issues.	Requires further evaluation for different use cases.	Enhances efficiency in vaccine safety protection.
[10]	Traceable Anonymous Transaction Protocol	Introduces TRCT, a traceable anonymous transaction protocol for enhancing traceability in anonymous transactions.	Supports public verification of transaction traceability.	Prior works did not provide public verification of traceability.	Ensures traceability in anonymous cryptocurrency transactions.
[11]	BlockASP: Aspect-Oriented Model Checking for Blockchain	Proposes BlockASP, a blockchain model verification method using Aspect-Oriented Programming (AOP).	Enhances verification of dynamic behaviors in blockchain systems.	Traditional model-checking approaches face challenges in blockchain dynamics.	Strengthens security and reliability in blockchain systems.
[12]	Blockchain-based Charging Payment with Privacy Preserving and Tracking Features	Introduces a blockchain-based, traceable, and privacy-preserving electric vehicle charging payment system.	Protects user identity confidentiality and transaction unlikability.	Existing solutions may hinder electricity regulators' investigations.	Balances privacy and traceability in electric vehicle charging payments.
[13]	Blockchain with Consensus Algorithm for TDMA-based Tactical Wireless Networks	Suggests a blockchain technology for tactical wireless networks based on TDMA that includes a timeslot allocation mechanism and consensus algorithm.	Offers decentralized data storage and efficient resource allocation.	Requires resource-efficient consensus algorithms for wireless networks.	Expands blockchain application in wireless network environments.

[14]	PBidm: Blockchain-based Identity Management for IIoT with Privacy Preserving Features	Presents PBidm, an identity management system for IIoT based on blockchain technology that protects privacy.	Supports traceability, revocability, unforgeability, blindness, unlikability, and public verifiability.	Existing schemes may be too anonymous or centralized.	Enhances identity privacy in Industrial Internet of Things (IIoT).
[15]	Distributed Data Sharing in e-health with Selective Likability and Traceability	Introduces a circulated data-sharing organization for e-health with selective likability and traceability.	Supports anonymity, accountability, likability, traceability, access control, and distributed storage.	Existing schemes lack fine-grained functionalities and rely on centralized storage.	Enhances data sharing capabilities in e-health while preserving privacy.
[16]	Asymmetric Fingerprinting for Media Sharing Blockchain	Presents a blockchain network for media sharing featuring user-side embedding and asymmetric fingerprinting.	Offers superior owner-side efficiency and TTP-free operation.	Existing works may not consider sharing needs and illegal redistribution.	Enhances privacy and traceability in decentralized media sharing.

Table 1. Analysis of existing tracing methods

The exploration of traceability extends to onsite construction activities (OCAs) in [5]. The research introduces a novel framework that combines computer vision and blockchain technologies to achieve traceability of OCAs. Cutting-edge deep learning algorithms are utilized to automatically retrieve OCA data from security footage, which is then documented in a blockchain consortium system. The results highlight the feasibility of this framework in ensuring The OCA information's veracity and clarity sets. In [6], the study addresses the evolving demands for privacy protection in public key infrastructure (PKI). It presents a PKI-based traceable self-randomization certificate authentication system., which balances user anonymity and traceability. This scheme allows users to randomize attributes for different scenarios while maintaining security and performance levels.

In the context of refurbished medical devices, [7] presents an NFT-based solution to manage and certify the gadgets' quality and safety. Dynamic composable NFTs are introduced as digital representations of medical devices, incorporating replacement parts and certificate documents. This approach enhances buyer confidence and safety while leveraging the Interplanetary File System for metadata storage sets. The integration of blockchain technology into Electronic Medical Records (EMRs) is explored in [8]. The research focuses on decentralized, trackable anonymous remote health care data sharing over a consortium blockchain process. It introduces an improved proxy re-encryption mechanism for fine-grained access control and privacy protection, leading to a more efficient data-sharing process.

Vaccine safety protection is addressed in [9], with the proposal of an improved, storage-efficient blockchain-based scheme. The system leverages cloud and cryptographic mechanisms to protect vaccine circulation data, offering efficiency and scalability benefits. Anonymous cryptocurrencies and their implications are discussed in [10]. The study introduces EPoK, a traceable anonymous transaction protocol mechanism called TRCT, and a partially extractable zero-knowledge proof scheme. By preserving anonymity and guaranteeing public verification of transaction traceability, these technologies raise security standards.

Blockchain's role in enhancing security and reliability in blockchain systems is highlighted in [11]. The research introduces Blockchain model checking can be improved with the use of aspect-oriented programming, or AOP. BlockASP, a technique for blockchain model verification that uses AOP to track and analyse dynamic behavior, is introduced to strengthen security and reliability levels. The article in [12] offers a blockchain-based charge payment system that is traceable and protects privacy (PTB-CP) for electric vehicles (EVs). This scheme protects users' identity confidentiality and un-likability of transactions while permitting the tracking of abnormal transactions, ensuring reliability and authentication sets. In [13], a blockchain system for tactical wireless networks based on TDMA that has a timeslot allocation strategy and consensus algorithm is proposed. The system offers advantages including traceability, tamper resistance, audibility levels, and decentralization. It allocates timeslots based on blockchain management contributions, reducing energy waste sets.

Work in [14] introduces PBidm, a blockchain-based identity management system that protects anonymity for IIoT scenarios. It supports [15, 16] blindness, traceability, revocability, unlikability, unforgeability, and public verifiability while addressing privacy concerns and minimizing the risk of a single point of failure set. Work in [17] presents a secure and low-cost distributed storage scheme for firefighting Internet of Things (IoT) data. It combines blockchain, IPFS, and PBFT consensus to enhance data security and traceability in fire scene investigations & scenarios.

Work in [18] introduces SPDL, a blockchain-secured and privacy-preserving decentralized learning system, addressing the need for efficient coordination, data privacy, and Byzantine fault tolerance in a decentralized machine learning process. Work in [19] proposes a blockchain-enabled dynamic application block generation (DABG) approach for the IoT., ensuring data security, dynamic device management, and restrictive traceability in a dynamic IoT system process. Work in [20] presents Eunomia, an anonymous and secure Vehicular Digital Forensics (VDF) scheme based on blockchain, which protects privacy, evidence accountability, access control, and traceability in IoV scenarios.

Work in [21] introduces dRAIN, a distributed Reliable Architecture for IoT Networks using directed acyclic graphs (DAGs) to provide resilience, reliability, and traceability in IoT networks without the scalability limitations of traditional blockchains. Work in [22] proposes BDIVE, a blockchain-supported authentication protocol for Drone-assisted IoV, ensuring security, traceability, and energy efficiency in the context of drone integration into IoV scenarios. Work in [23] addresses security issues in the metaverse's ubiquitous access controls (UACs) by proposing a blockchain-based multi-signature lock for UAC (BMSL-UAC) scheme that ensures data access control and traceability sets.

Work in [24] introduces a blockchain-assisted reputation mechanism for Distributed Cloud Storage (DCS) to promote service success rate, efficiency, and security by quantifying CSP reputations and considering storage resource capacity levels. Work in [25] presents a blockchain-based protocol for Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) authentication in VANETs, addressing computation overhead, traceability, and resistance to attacks.

Work in [26] proposes a blockchain-based solution for transparent, traceable, trusted, and decentralized academic ranking systems, addressing transparency, trust, and centralization issues in existing ranking systems. Work in [27] introduces AT-DS-VAHN, an accountable attribute-based data-sharing scheme with blockchain technology for VANETs, ensuring traceability and efficient user revocation while maintaining security and privacy levels. Work in [28] presents EBCPA, an efficient blockchain-based conditional privacy-preserving authentication (BCPPA) protocol for VANETs, reducing verification and traceability overhead while maintaining security and privacy levels. Work in [29] introduces BHTE, a Blockchain-based Hierarchical Trust Evaluation strategy for 5G-enabled Intelligent Transportation Systems (5G-ITS), providing trust storage and verification through federated deep learning and incentives for different use cases.

Work in [30] designs a blockchain-supported framework for V2V and V2R transaction management, ensuring secure data exchange, bandwidth optimization, and decentralized payment in vehicular networks. Work in [31] proposes BTDPI, a privacy-preserving traceable DPI system for blockchain-based Industrial Internet of Things (IIoT), addressing encrypted traffic inspection and traceability challenges. Work in [32] introduces PCHA, a policy-based chameleon hash with black box accountability for controlled blockchain rewriting, ensuring traceability and accountability in blockchain modifications.

Reference Number	**Method Name**	**Findings**	**Advantages**	**Limitations**	**Impacts**
[17]	Secure IoT Data Storage with Blockchain	Blockchain-based storage scheme for firefighting IoT data.	Reduced storage space overhead, improved throughput, and lower latency.	Limited to firefighting IoT data storage. Dependency on	Enhances fire accident traceability and data security.

			Ensures data security and traceability.	blockchain technology.	
[18]	Privacy-Preserving Decentralized Learning	SPDL combines differential privacy, blockchain, and Byzantine Fault-Tolerant (BFT) consensus.	Efficient decentralized learning with Byzantine fault tolerance and data privacy, transparency, and traceability.	Complex integration of various technologies. Lack of scalability may affect performance.	Operative and efficient decentralized learning with strong security and privacy guarantees.
[19]	Dynamic Blockchain for IoT with Conditional Trace	Dynamic application blockchain-enabled Internet of Things block creation technique with dynamic device management.	Achieves non-frameability, traceability, and anonymity. Manages devices dynamically while maintaining data security and user privacy.	Specific to IoT applications. Requires consortium blockchain.	Efficient management of IoT devices with conditional traceability and data security.
[20]	Anonymous Vehicular Digital Forensics	Eunomia is a blockchain-based, anonymous, and secure VDF scheme.	Use decentralized anonymous credentials to protect privacy. Achieves fine-grained evidence access control and traceability.	Complex cryptographic operations may affect performance.	Ensures privacy, access control, and traceability in vehicular digital forensics.
[21]	Reliable Architecture for IoT Networks	dRAIN: a distributed Reliable Architecture for IoT Networks.	Provides resilience, reliability, and traceability in IoT networks. Overcomes limitations of classical DLTs.	Limited scalability and high cost of classical DLTs. May require significant adoption changes.	Ensures reliability and traceability in IoT networks.
[22]	Blockchain-supported Authentication for IoV	BDIVE: Blockchain-supported authentication protocol for Drone-assisted IoV.	Provides energy-efficiency, traceability, and accountability. Reduces energy consumption and computational cost.	Extensive testing required for practical implementation. May introduce some overhead.	Enhances security and efficiency in drone-assisted IoV.
[23]	Blockchain-based Multisignature Lock for UAC	BMSL-UAC: a blockchain-based multisignature lock for UAC scheme.	Ensures authorized data access and full life-cycle data management with traceability.	May require integration into existing systems. Some resource consumption and latency.	Enhances UAC security and data management in the metaverse.
[24]	Blockchain-assisted	Blockchain-assisted reputation	Ensures tamper-proof reputation evaluation for cloud	Complexity in calculating CSPs' survival probability.	Enhances reputation evaluation and

	Reputation for Distributed CS	mechanism for DCS.	service providers. Promotes service success and security.	May need integration into existing systems.	security in distributed cloud storage.
[25]	Blockchain-based V2I and V2V Authentication	Blockchain-based protocol for V2I and V2V authentication.	Achieves lightweight authentication with anonymity and traceability. Uses Physically Unclonable Functions (PUF) technology.	Requires integration into VANET infrastructure. Some computational cost.	Enhances authentication efficiency and security in VANETs.
[26]	Transparent, Traceable, and Decentralized Rankings	Decentralized, transparent, and traceable academic ranking systems using blockchain technology.	Provides transparency, traceability, trust, and decentralization in academic ranking systems.	Potential concerns about blockchain overhead and integration.	Enhances transparency and trust in academic ranking systems.
[27]	Accountable Attribute-based Data Sharing with B	Accountable attribute-based data sharing using blockchain technology is known as AT-DS-VAHN.	Achieves distributed key storage, traceability, and efficient user revocation in VANETs.	Requires integration into VANET infrastructure. Some complexity in key management.	Enhances data sharing security and efficiency in VANETs.
[28]	Efficient Blockchain-based Conditional Privacy	EBCPA: More efficient BCPPA protocol for VANETs.	Reduces time cost of traceability and verification. Provides efficient conditional privacy protection.	May require integration into VANET infrastructure. Some computational cost.	Improves efficiency and privacy in VANETs.
[29]	Hierarchical Trust Evaluation for 5G-ITS	BHTE: Blockchain-based Hierarchical Trust Evaluation for 5G-ITS.	Utilizes federated deep learning and hierarchical incentives for trust evaluation in 5G-ITS.	Complexity in trust evaluation mechanisms. Requires integration into 5G-ITS infrastructure.	Enhances trust and security in 5G-ITS.
[30]	Blockchain-based V2V and V2R Transaction Framework	Blockchain-based framework for V2V and V2R transaction framework.	Ensures security and scalability in data exchange and bandwidth transactions in vehicular networks.	Requires integration into the vehicular network infrastructure. May introduce some overhead.	Enhances service quality and decentralized payment in vehicular networks.
[31]	Privacy-Preserving DPI in Blockchain-based IIoT	BTDPI: Privacy-preserving traceable DPI system for encrypted traffic	Efficiently carries out traffic encryption inspection. Provides identity traceability mechanism.	Some computational overhead in the traceability mechanism. Requires integration	Enhances security and traceability in blockchain-based IIoT.

		in blockchain-based IIoT.		into IIoT infrastructure.	
[32]	Blockchain with Controlled Rewriting	PCHA: A blockchain-based controlled rewriting mechanism with blackbox accountability.	Allows controlled rewriting with linkability and traceability. Offers accountability for trapdoor holders.	May introduce complexity in blockchain operations. Requires integration into existing blockchain systems.	Provides controlled rewriting while maintaining accountability in blockchains.

Table 2. Deep Learning & Machine Learning based Analysis Methods

Work in [33] presents a blockchain-empowered publish/subscribe (P/S) scheme for secure video sharing in vehicular edge computing (VEC), offering fine-grained access control and traceability levels. Work in [34] introduces PEATS, a blockchain-based system for administrative punishment in market supervision, addressing data access permission abuse and timeliness issues while ensuring traceability and transparency levels.Work in [35] focuses on the use of blockchain for vehicle reputation management in the context of Internet of Vehicles (IoV). It introduces the R-tracing scheme, which incorporates a vehicle reputation model and a consortium blockchain-based system. The model includes mechanisms for reward, punishment, and regular taxation to encourage vehicles to report information accurately. The system involves multiple organizations and abstracts reputation update tasks into transactions. Extensive simulations and performance evaluations demonstrate the effectiveness of R-tracing in resisting attacks and improving throughput compared to existing schemes. Work in [36] addresses the need for secure indoor contact tracing under the framework of the COVID-19 outbreak. We suggest the TB-ICT architecture as a reliable blockchain-enabled approach. It makes use of randomized hash windows (W-Hash), dynamic Proof-of-Work (dPoW), and dynamic Proof-of-Credit (dPoC) techniques. to ensure data privacy and integrity sets. The framework also leverages IoT indoor localization infrastructures for an accurate contact tracing process.

Work in [37] deals with the issue of tracing illicit financial flows in blockchain transactions. It presents TRacer, an intelligent transaction tracing tool based on a graph search approach. TRacer is designed to work with multiple account-based blockchain platforms and can handle complex transaction behavior in decentralized finance (DeFi). It offers efficient and effective tracing of fund transfers, outperforming existing methods. Work in [38] introduces the MyDataChain framework, which enhances OAuth-based data portability schemes with blockchain technology. The framework uses smart contracts to facilitate authentication and authorization processes, ensuring data integrity and privacy. It employs Non-Interactive Zero-Knowledge (NIZK) schemes to protect user privacy while achieving data portability levels.

Work in [39] addresses the performance limitations of blockchain sharding caused by imbalanced transaction loads on different shards. LB-Chain is proposed as a novel sharding system that dynamically balances transaction loads by migrating active accounts between shards. Extensive experiments demonstrate significant improvements in transaction confirmation delays and throughput levels.

Work in [40] discusses privacy-preserving identity management using blockchain technology. It proposes a PPIdM system that allows users to manage their identity attributes while keeping their real identities hidden from all entities. The system ensures traceability and security while preserving user privacy levels. Work in [41] focuses on securing access controls in the metaverse using blockchain-based multisignature locks. It introduces the BMSL-UAC scheme, which enables data access control and traceability in the metaverse scenarios. The scheme utilizes a consortium blockchain system to manage user data access behaviors.

Reference Number	**Method Name**	**Findings**	**Advantages**	**Limitations**	**Impacts**
[33]	Blockchain-Powered Secure Video Sharing in VEC	Proposed a blockchain-based publish/subscribe scheme for secure video sharing in VEC.	Enhances data security and privacy in vehicular edge computing.	Data security and privacy concerns can limit video sharing.	Enables real-time video streaming and user self-certification.

[34]	Punishment Supervisor (PEATS) for Administrative Punishment	Introduced PEATS, a blockchain-based system for administrative punishment.	Prevents abuse of data access permission and ensures timeliness in punishment.	It may have a slight impact on system throughput and latency.	Provides traceability, transparency, and timeliness assurance.
[35]	Blockchain-Based Consortium System for Vehicle Reputation Management	Proposed A blockchain-based vehicle reputation management system called R-tracing scheme.	Encourages vehicles to actively report information and manages multi-party participation.	The effectiveness of R-tracing needs to be verified through simulation experiments.	Resists malicious attacks and selfish behavior, achieving high throughput.
[36]	Reliable Blockchain-Powered Indoor CT System	Introduced TB-ICT, an indoor contact tracking system powered by blockchain technology.	Protects confidentiality and accuracy of CT data in indoor environments.	The field of indoor CT is still in its infancy.	Prevents the spread of COVID-19 within enclosed spaces.
[37]	TRacer: Intelligent Transaction Tracing in Blockchain	Presented TRacer, an intelligent transaction tracing tool for blockchain.	Efficiently traces fund transfers on transaction graphs.	Current tracing methods have limitations.	Efficiently traces blockchain transactions with lower costs.
[38]	MyDataChain: Blockchain-Enhanced Data Portability	Proposed MyDataChain, a blockchain-based framework for data portability.	Enhances data portability and privacy while resolving disputes.	No interactions specified between authorization server and resource server in OAuth.	Provides a feasible privacy-preserving means of data portability.
[39]	LB-Chain: Load-Balanced Sharding in Blockchain	Introduced LB-Chain, a sharding system with dynamic load balancing.	Addresses performance degradation in sharded blockchains.	Sharding can achieve limited throughput improvement.	Significantly reduces transaction confirmation delays.
[40]	Privacy-Preserving Identity Management on Blockchain	Proposed a PPIdM system on the blockchain to protect user privacy.	Preserves user privacy and ensures malicious users are traceable.	Existing PPIdM systems rely on identity providers, which can compromise privacy.	Allows users to manage identity attributes while protecting privacy.
[41]	Blockchain-Based Multisignature Lock for UAC (BMSL-UAC)	Introduced BMSL-UAC, a blockchain-based multisignature lock for UAC.	Ensures data access control and traceability in the metaverse.	Numerous threats exist in the access layer of the metaverse.	Provides secure access control and traceability in the metaverse.
[42]	Blockchain-Based Aviation Supplier	Proposed a blockchain-based platform for sharing	Integrates manufacturing quality management with	Challenges include technological	Provides data-sharing solutions for aviation

	Manufacturing Data-Sharing	aviation supplier data.	blockchain technology.	issues in the aviation sector.	product quality data.
[43]	Accountable Fine-Grained Blockchain Rewriting	Introduced Responsibly doing fine-grained blockchain rewriting in a permissionless environment.	Enhances blockchain rewriting with accountability in open blockchains.	Traditional blockchain fund tracing methods are heuristic and lack efficiency.	Provides a means for accountable blockchain rewriting.
[44]	Eunomia: Anonymous and Secure Vehicular Digital Forensics	Proposed Eunomia is a blockchain-based, anonymous, and secure VDF scheme.	Conserves privacy and evidence accountability in vehicular investigations.	Protecting privacy and evidence accountability is challenging in VDF.	Achieves strong privacy and security properties in VDF.
[45]	Blockchain in Agriculture: Challenges and Opportunities	Conducted a review of 152 scientific works on the application of blockchain in agriculture.	Identified challenges and open issues in applying blockchain in agriculture.	Blockchain can introduce complexity in agriculture systems.	Offers potential for innovative solutions in agriculture.
[46]	Blackbox Accountability for Policy-Based Chameleon Hash	Introduced blackbox accountability for policy-based chameleon hash in blockchain.	Enhances blockchain rewriting with accountability in permissionless settings.	Existing blockchain immutability hinders blockchain development.	Provides an efficient solution for controlled blockchain rewriting.
[47]	Blockchain-Assisted Safe Multi-UAV Task Distribution	Proposed B-UAVM, a blockchain-supported multi-UAV task management scheme.	Ensures entity identity and task data security in UAV networks.	Current approaches rely on centralized authentication, which creates a single point of failure.	Enhances safety and efficiency in multi-UAV scenarios.
[48]	Auditable Semi-Asynchronous Federated Learning using Blockchain Technology	Introduced BASA-FL, a blockchain-based federated learning system with auditing.	Addresses trust issues and resource efficiency challenges in federated learning.	Traditional federated learning lacks a mutual consensus auditing mechanism.	Provides traceability, auditability, and quantification of contributions in FL.
[49]	Reliable Source for Information on Counterfeiting in ADS-B	Proposed a dependable service plan for ADS-B system data that prevents counterfeiting.	Ensures the authenticity and integrity of ADS-B information using blockchain.	ADS-B lacks security authentication and information integrity protection.	Protects ADS-B information from tampering and data leakage.
[50]	Efficient Threshold Attribute-Based	Presented an efficient threshold attribute-based anonymous credential scheme.	supports the revocation of credentials and	Coconut has linear complexities in	Reduces computational and communication

	Anonymous Credentials		threshold tracing of user identities..	credential verification.	complexities in FL.

Table 3. Iterative Methods for Tracing Blockchains

Work in [42] presents an aircraft quality data-sharing platform for suppliers in the production process powered by blockchain. It integrates quality control in the manufacturing supply chain using blockchain technology to protect and maintain data integrity in the aviation industry sets. Work in [43] presents permissionless fine-grained blockchain rewriting that is responsible. It proposes a framework for secure blockchain rewriting and presents a concrete construction with accountability features.

Work in [44] discusses the importance of Vehicular Digital Forensics (VDF) and proposes Eunomia, a blockchain-based, safe, and anonymous VDF scheme technology set. Eunomia ensures privacy, evidence accountability, VDF, access control, and traceability investigations & operations. Work in [45] explores the application of blockchain in agriculture to enhance supply chain management and traceability sets. It reviews 152 scientific works and identifies challenges and open issues in applying blockchain to agriculture scenarios.

Work in [46] addresses the challenge of blockchain immutability and proposes a design for a redactable blockchain with black box accountability. The design offers a controlled way to break blockchain immutability while holding trapdoor holders accountable for their actions. Work in [47] focuses on securing UAV swarm networks using blockchain technology. It introduces the B-UAVM scheme, which ensures entity identity and task data security in UAV formations. The scheme uses a three-layer blockchain structure and consensus mechanisms for secure UAV task management sets. Work in [48] addresses challenges in federated learning (FL) and proposes the BASA-FL system, which uses blockchain for auditing FL processes and offers semi-asynchronous coordination sets. It quantifies worker contributions and distributes rewards based on their performance levels. Work in [49] discusses the security issues in the Automatic Dependent Surveillance-Broadcast (ADS-B) system and proposes a blockchain-based solution to protect ADS-B information from tampering and unauthorized access. Work in [50] presents a threshold attribute-based credentials scheme suitable for decentralized systems like blockchains. It offers selective disclosure, user identity tracking, and account credential revocation, addressing trust and efficiency challenges in the federated learning process. These research works cover a wide range of applications and security challenges related to blockchain technology, demonstrating its versatility and potential across various domains. Next, we discuss the efficiency of these models in terms of different evaluation metrics and compare them with individual model sets.

4. Result & Analysis

In this section we comprehensive overview of various research works related to blockchain technology and its applications in different domains. Each entry in table 4 corresponds to a specific research paper or work, and it provides essential information about the methodology used, efficiency in terms of energy and tracing, deployment cost, delay, and scalability of the proposed solutions. Below is a breakdown of the key elements in the table:

- **Method Name:** This column briefly describes the methodology or approach used in each research work. It provides insight into the specific focus or application area of blockchain technology.
- **Energy Efficiency:** This column assesses the energy efficiency of the proposed solutions. It categorizes the efficiency into various levels, including Very Low (VL), Low (L), Medium (M), and Very High (VH). This assessment helps in understanding the environmental impact and resource requirements of each method.
- **Tracing Efficiency:** Tracing efficiency evaluates how effectively the blockchain technology can trace and verify transactions or data. It is categorized as Very Low (VL), Low (L), Medium (M), and Very High (VH). This parameter is crucial for applications where traceability and authenticity are paramount.
- **Deployment Cost:** Deployment cost indicates the financial resources required to implement the proposed blockchain solution. It is categorized as Very Low (VL), Low (L), Medium (M), and Very High (VH). Understanding the cost implications is vital for practical adoption.
- **Delay:** Delay measures the time it takes for transactions or data to be processed within the blockchain system. It is categorized as Very Low (VL), Low (L), Medium (M), and Very High (VH). Lower delay is often preferred, especially in real-time applications.
- **Scalability:** Scalability assesses how well the blockchain system can handle an increasing number of transactions or users. It is categorized as Very Low (VL), Low (L), Medium (M), and Very High (VH). Scalability is critical for widespread adoption and system performance levels.

Reference Number	Method Name	Energy Efficiency	Tracing Efficiency	Deployme nt Cost	De lay	Scala bility
[1]	Blockchain-based Supply Chain Traceability	M	VH	VL	V H	L
[2]	Blockchain Service for Information Traceability	H	H	L	V H	VH
[3]	Dynamic Trust-based Redactable Blockchain	L	H	VH	VL	VL
[4]	Blockchain Traceability in Agriculture Supply Chain	M	H	VL	M	M
[5]	Traceability of Onsite Construction Activities	L	L	L	V H	VH
[6]	Traceable Self-randomization Certificate Authentication	M	VH	L	H	VL
[7]	An NFT-based Approach to the Management of Refurbished Medical Equipment	L	H	VL	V H	VH
[8]	Trackable Anonymous Remote Healthcare Data Sharing	VH	H	VL	L	VH
[9]	Storage-efficient Vaccine Safety Protection	L	L	VH	V H	L
[10]	Traceable Anonymous Transaction Protocol	VL	VH	VH	L	L
[11]	BlockASP: Aspect-Oriented Model Checking for Blockchain	VL	H	M	VL	H
[12]	Blockchain-based Charging Payment with Privacy Preserving and Tracking Features	H	VH	L	H	VH
[13]	Blockchain with Consensus Algorithm for TDMA-based Tactical Wireless Networks	L	H	H	VL	VH
[14]	PBidm: Blockchain-based Identity Management for IIoT that Preserves Privacy	VL	M	M	VL	M
[15]	Distributed Data Sharing in e-health with Selective Likability and Traceability	L	M	H	H	VH
[16]	Asymmetric Fingerprinting for Media Sharing Blockchain	L	VH	VH	H	L
[17]	Secure IoT Data Storage with Blockchain	L	H	L	L	L
[18]	Privacy-Preserving Decentralized Learning	VL	H	L	M	VH
[19]	Dynamic Blockchain for IoT with Conditional Trace	H	M	H	VL	L
[20]	Anonymous Vehicular Digital Forensics	H	VL	VH	VL	VH
[21]	Reliable Architecture for IoT Networks	VL	L	H	H	VH
[22]	Blockchain-supported Authentication for IoV	M	L	M	V H	L
[23]	Blockchain-based Multisignature Lock for UAC	L	H	VH	L	L

[24]	Blockchain-assisted Reputation for Distributed CS	VH	VH	VL	H	L
[25]	Blockchain-based V2I and V2V Authentication	M	VL	L	V H	VL
[26]	Transparent, Traceable, and Decentralized Rankings	H	M	VH	V H	VH
[27]	Accountable Attribute-based Data Sharing with B	H	H	L	V H	VL
[28]	Efficient Blockchain-based Conditional Privacy	L	L	L	V H	H
[29]	Hierarchical Trust Evaluation for 5G-ITS	M	M	VL	H	M
[30]	Blockchain-based V2V and V2R Transaction Framework	VL	VL	M	H	M
[31]	Privacy-Preserving DPI in Blockchain-based IIoT	M	M	H	V H	VL
[32]	Blockchain with Controlled Rewriting	M	L	M	V H	M
[33]	Blockchain-Powered Secure Video Sharing in VEC	M	M	VL	L	L
[34]	Punishment Supervisor (PEATS) for Administrative Punishment	L	H	VL	L	H
[35]	Consortium Blockchain-Based Vehicle Reputation Management	L	VH	VL	V H	L
[36]	Trustworthy Blockchain-Enabled System for Indoor CT	H	H	H	VL	VH
[37]	TRacer: Intelligent Transaction Tracing in Blockchain	M	VH	H	M	VH
[38]	MyDataChain: Blockchain-Enhanced Data Portability	VH	L	H	L	H
[39]	LB-Chain: Load-Balanced Sharding in Blockchain	VL	M	L	M	VL
[40]	Privacy-Preserving Identity Management on Blockchain	H	VL	H	L	VH
[41]	Mult signature Lock for UAC Using Blockchain Technology (BMSL-UAC)	VH	VL	VH	VL	M
[42]	Blockchain-Based Aviation Supplier Manufacturing Data-Sharing	VL	VL	L	L	H
[43]	Accountable Fine-Grained Blockchain Rewriting	H	M	VH	V H	VL
[44]	Eunomia: Anonymous and Secure Vehicular Digital Forensics	H	M	M	H	VL
[45]	Blockchain in Agriculture: Challenges and Opportunities	VL	M	L	V H	VL

[46]	Blackbox Accountability for Policy-Based Chameleon Hash	H	M	VL	H	VL
[47]	Blockchain-Supported Secure Multi-UAV Task Management	M	VL	M	M	L
[48]	Blockchain-based Auditable Semi-Asynchronous Federated Learning	VL	VL	L	VL	H
[49]	Reliable Source for Information on Counterfeiting in ADS-B	M	M	VL	H	L
[50]	Efficient Threshold Attribute-Based Anonymous Credentials	VL	H	VH	VL	L

Table 4. Empirical Evaluation of different Blockchain Analysis Methods

Based on the evaluation, the following observations can be made for different methods,

Energy Efficiency:

- Notably, method [35], which focuses on the "Traceability of Onsite Construction Activities," exhibits low energy efficiency. On the contrary, methods [13] ("Blockchain with Consensus Algorithm for TDMA-based Tactical Wireless Networks") and [21] ("Reliable Architecture for IoT Networks") demonstrate higher energy efficiency, making them more sustainable options in scenarios where energy conservation is crucial.

Tracing Efficiency:

- Method [43] ("Accountable Fine-Grained Blockchain Rewriting") stands out with very high tracing efficiency, offering robust tracing capabilities. Method [16] ("Asymmetric Fingerprinting for Media Sharing Blockchain") also excels in this regard, offering efficient tracing mechanisms. Conversely, [29] ("Hierarchical Trust Evaluation for 5G-ITS") and [10] ("Traceable Anonymous Transaction Protocol") exhibit lower tracing efficiency.

Deployment Cost:

- Method [2] ("Blockchain Service for Information Traceability") presents a low deployment cost, making it an attractive option for cost-conscious implementations. On the other hand, method [48] ("Blockchain-based Auditable Semi-Asynchronous Federated Learning") and [3] ("Dynamic Trust-based Redactable Blockchain") may require higher initial investments due to their advanced features and capabilities.

Delay:

- [33] ("Blockchain-Powered Secure Video Sharing in VEC") demonstrates low delay, making it suitable for real-time applications. Conversely, method [14] ("PBidm: Privacy-preserving Blockchain-based Identity Management for IIoT") exhibits higher delay characteristics, which may not be suitable for latency-sensitive use cases.

Scalability:

- Method [38] ("MyDataChain: Blockchain-Enhanced Data Portability") and [19] ("Dynamic Blockchain for IoT with Conditional Trace") exhibit scalability advantages, making them well-suited for applications requiring the ability to scale efficiently. In contrast, methods like [11] ("BlockASP: Aspect-Oriented Model Checking for Blockchain") and [46] ("Blackbox Accountability for Policy-Based Chameleon Hash") may face challenges related to scalability.

Overall Assessment:

- Considering the various dimensions, method [43] ("Accountable Fine-Grained Blockchain Rewriting") emerges as a strong contender due to its high tracing efficiency and versatility. It offers a robust solution for applications requiring accountable blockchain rewriting.
- Method [35] ("Traceability of Onsite Construction Activities") excels in Energy Efficiency but may not be the best choice for applications requiring efficient tracing or low delay.
- For cost-effective implementations, method [2] ("Blockchain Service for Information Traceability") offers a viable solution.
- Methods [38] ("MyDataChain: Blockchain-Enhanced Data Portability") and [19] ("Dynamic Blockchain for IoT with Conditional Trace") exhibit good scalability characteristics, making them suitable for applications demanding scalability.
- Method [33] ("Blockchain-Powered Secure Video Sharing in VEC") is well-suited for real-time scenarios with low delay requirements.

In conclusion, the choice of the most suitable method depends on the specific requirements and priorities of the application, such as energy efficiency, tracing capabilities, cost constraints, delay tolerance, and scalability needs.

5. Conclusion & Future Scopes

In conclusion, the extensive analysis of the various blockchain-based methods presented in the provided observations reveals a rich landscape of solutions designed to address a wide spectrum of challenges and opportunities across diverse domains. Each method carries its own set of advantages and limitations, making them suitable for specific use cases and shedding light on the broader impacts of blockchain technology on various industries.

Blockchain technology has showcased its potential in improving time efficiency in supply chain traceability ([1]) and ensuring information traceability and protection ([2]), impacting supply chain transparency and the broader application of blockchain technology in different domains.

Dynamic trust-based redactable blockchains ([3]) have emerged as a significant advancement in ensuring full-process security with pre-modification pre-evaluation, thereby enhancing security and traceability in redactable blockchains.

The integration of computer vision and blockchain for onsite construction traceability ([5]) exemplifies the synergy of cutting-edge technologies to improve construction process quality and transparency.

Methods such as traceable self-randomization certificate authentication ([6]) and NFT-based solutions for managing refurbished medical devices ([7]) contribute to enhancing privacy, traceability, and trust in their respective domains.

Blockchain technology has also made substantial contributions to the healthcare sector, exemplified by the trackable anonymous remote healthcare data sharing scheme ([8]), which strikes a balance between privacy and traceability in healthcare data sharing.

Efficiency improvements in vaccine safety protection ([9]) and traceable anonymous transaction protocols ([10]) are significant steps forward in addressing critical issues within their respective domains.

The innovative approach of BlockASP ([11]) enhances security and reliability in blockchain systems by leveraging Aspect-Oriented Programming (AOP) for dynamic behavior verification.

Furthermore, blockchain-supported solutions for vehicular networks ([20], [22], [25], [30], [35]) have had a substantial impact on improving authentication, security, and scalability in vehicular environments.

In the realm of privacy-preserving solutions, blockchain-based identity management for IIoT ([14]), distributed data sharing in e-health ([15]), and privacy-preserving decentralized learning ([18]) have demonstrated significant strides in preserving user privacy and enhancing data security.

Blockchain technology has also influenced data storage, as seen in the cases of secure IoT data storage ([17]), load-balanced sharding ([39]), and blockchain-enhanced data portability ([38]), all contributing to efficiency improvements in their respective domains.

Additionally, innovative approaches like blackbox accountability for controlled blockchain rewriting ([32], [43], [46]) provide means for enhancing accountability and controlled rewriting while maintaining transparency in blockchain systems.

In the context of specific domains, blockchain has shown promise in revolutionizing agriculture supply chains ([4]), improving reputation evaluation in distributed cloud storage ([24]), and ensuring authenticity and integrity in the ADS-B system ([49]).

In conclusion, the collective impact of these blockchain-based methods is poised to shape diverse industries and domains by addressing critical challenges, enhancing security, improving transparency, and preserving privacy. As the blockchain ecosystem continues to evolve, it offers a wealth of opportunities for further innovation and application, underlining its potential as a transformative technology in various sectors. This comprehensive analysis underscores the significance of blockchain technology in advancing solutions for complex real-world problems and highlights the need for continued research and development in this dynamic field for different use cases.

Future Scope

The future scope of this paper holds great promise for further exploration and innovation in the realm of blockchain-based methods. As the technology continues to evolve, researchers and practitioners can delve deeper into optimizing energy-efficient solutions, fine-tuning tracing efficiency mechanisms, and developing cost-effective deployment strategies tailored to specific industries and applications. Additionally, there is ample room for enhancing scalability and reducing delays, especially in real-time systems. Further research into blockchain integration with cutting-edge technology like artificial intelligence, Internet of Things (IoT), and edge computing can unlock new avenues for solving complex challenges across domains such as supply chain management, healthcare, and vehicular networks. Moreover, the ongoing refinement of privacy-preserving techniques and the exploration of novel consensus algorithms hold substantial potential for safeguarding user privacy and data security levels. The future of blockchain-based solutions lies in their adaptability to diverse contexts, and this paper paves the way for exciting developments in the blockchain landscapes.

References

[1] H. Wu, S. Jiang and J. Cao, "High-Efficiency Blockchain-Based Supply Chain Traceability," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 4, pp. 3748-3758, April 2023, doi: 10.1109/TITS.2022.3205445.

[2] P. Zhu, J. Hu, X. Li and Q. Zhu, "Using Blockchain Technology to Enhance the Traceability of Original Achievements," in IEEE Transactions on Engineering Management, vol. 70, no. 5, pp. 1693-1707, May 2023, doi: 10.1109/TEM.2021.3066090.

[3] Y. Zhang, Z. Ma, S. Luo and P. Duan, "Dynamic Trust-Based Redactable Blockchain Supporting Update and Traceability," in IEEE Transactions on Information Forensics and Security, vol. 19, pp. 821-834, 2024, doi: 10.1109/TIFS.2023.3326379.

[4] P. Saranya and R. Maheswari, "Proof of Transaction (PoTx) Based Traceability System for an Agriculture Supply Chain," in IEEE Access, vol. 11, pp. 10623-10638, 2023, doi: 10.1109/ACCESS.2023.3240772.

[5] H. Wu, H. Li, X. Luo and S. Jiang, "Blockchain-Based Onsite Activity Management for Smart Construction Process Quality Traceability," in IEEE Internet of Things Journal, vol. 10, no. 24, pp. 21554-21565, 15 Dec.15, 2023, doi: 10.1109/JIOT.2023.3300076.

[6] Y. Zhu et al., "tsrCert: Traceable Self-Randomization Certificate and Its Application to Blockchain Supervision," in Tsinghua Science and Technology, vol. 28, no. 6, pp. 1128-1147, December 2023, doi: 10.26599/TST.2023.9010053.

[7] S. A. Gebreab, K. Salah, R. Jayaraman and J. Zemerly, "Trusted Traceability and Certification of Refurbished Medical Devices Using Dynamic Composable NFTs," in IEEE Access, vol. 11, pp. 30373-30389, 2023, doi: 10.1109/ACCESS.2023.3261555.

[8] J. Liu et al., "Conditional Anonymous Remote Healthcare Data Sharing Over Blockchain," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 5, pp. 2231-2242, May 2023, doi: 10.1109/JBHI.2022.3183397.

[9] L. Cui, Z. Xiao, F. Chen, H. Dai and J. Li, "Protecting Vaccine Safety: An Improved, Blockchain-Based, Storage-Efficient Scheme," in IEEE Transactions on Cybernetics, vol. 53, no. 6, pp. 3588-3598, June 2023, doi: 10.1109/TCYB.2022.3163743.

[10] J. Duan, L. Wang, W. Wang and L. Gu, "TRCT: A Traceable Anonymous Transaction Protocol for Blockchain," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 4391-4405, 2023, doi: 10.1109/TIFS.2023.3296286.

[11] A. M. R. AlSobeh and A. A. Magableh, "BlockASP: A Framework for AOP-Based Model Checking Blockchain System," in IEEE Access, vol. 11, pp. 115062-115075, 2023, doi: 10.1109/ACCESS.2023.3325060.

[12] Y. Wu, C. Zhang and L. Zhu, "Privacy-Preserving and Traceable Blockchain-Based Charging Payment Scheme for Electric Vehicles," in IEEE Internet of Things Journal, vol. 10, no. 24, pp. 21254-21265, 15 Dec.15, 2023, doi: 10.1109/JIOT.2023.3283415.

[13] J. Lee and M. Lee, "A Blockchain System for TDMA-Based Tactical Wireless Networks With Constrained Resources," in IEEE Access, vol. 11, pp. 6857-6866, 2023, doi: 10.1109/ACCESS.2023.3237828.

[14] Z. Bao, D. He, M. K. Khan, M. Luo and Q. Xie, "PBidm: Privacy-Preserving Blockchain-Based Identity Management System for Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 19, no. 2, pp. 1524-1534, Feb. 2023, doi: 10.1109/TII.2022.3206798.

[15] Z. Bao, D. He, H. Wang, M. Luo and C. Peng, "A Group Signature Scheme With Selective Linkability and Traceability for Blockchain-Based Data Sharing Systems in E-Health Services," in IEEE Internet of Things Journal, vol. 10, no. 23, pp. 21115-21128, 1 Dec.1, 2023, doi: 10.1109/JIOT.2023.3284968.

[16] X. Xiao, Y. Zhang, Y. Zhu, P. Hu and X. Cao, "FingerChain: Copyrighted Multi-Owner Media Sharing by Introducing Asymmetric Fingerprinting Into Blockchain," in IEEE Transactions on Network and Service Management, vol. 20, no. 3, pp. 2869-2885, Sept. 2023, doi: 10.1109/TNSM.2023.3237685.

[17] L. Li, D. Jin, T. Zhang and N. Li, "A Secure, Reliable and Low-Cost Distributed Storage Scheme Based on Blockchain and IPFS for Firefighting IoT Data," in IEEE Access, vol. 11, pp. 97318-97330, 2023, doi: 10.1109/ACCESS.2023.3311712.

[18] M. Xu, Z. Zou, Y. Cheng, Q. Hu, D. Yu and X. Cheng, "SPDL: A Blockchain-Enabled Secure and Privacy-Preserving Decentralized Learning System," in IEEE Transactions on Computers, vol. 72, no. 2, pp. 548-558, 1 Feb. 2023, doi: 10.1109/TC.2022.3169436.

[19] S. Basudan, "A Scalable Blockchain Framework for Secure Transactions in IoT-Based Dynamic Applications," in IEEE Open Journal of the Communications Society, vol. 4, pp. 1931-1945, 2023, doi: 10.1109/OJCOMS.2023.3307337.

[20] M. Li, Y. Chen, C. Lal, M. Conti, M. Alazab and D. Hu, "Eunomia: Anonymous and Secure Vehicular Digital Forensics Based on Blockchain," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 1, pp. 225-241, 1 Jan.-Feb. 2023, doi: 10.1109/TDSC.2021.3130583.

[21] L. Petrosino, G. Pescetelli, Q. Fieramosca, S. D. Valle, M. Merone and L. Vollero, "dRAIN: A Distributed Reliable Architecture for IoT Networks," in IEEE Internet of Things Journal, vol. 11, no. 1, pp. 1746-

1760, 1 Jan.1, 2024, doi: 10.1109/JIOT.2023.3290822.

[22] M. A. El-Zawawy, A. Brighente and M. Conti, "Authenticating Drone-Assisted Internet of Vehicles Using Elliptic Curve Cryptography and Blockchain," in IEEE Transactions on Network and Service Management, vol. 20, no. 2, pp. 1775-1789, June 2023, doi: 10.1109/TNSM.2022.3217320.

[23] K. Gai, S. Wang, H. Zhao, Y. She, Z. Zhang and L. Zhu, "Blockchain-Based Multisignature Lock for UAC in Metaverse," in IEEE Transactions on Computational Social Systems, vol. 10, no. 5, pp. 2201-2213, Oct. 2023, doi: 10.1109/TCSS.2022.3226717.

[24] Q. Dong, J. Tang, S. Dang, G. Chen and J. A. Chambers, "Blockchain-Assisted Reputation Mechanism for Distributed Cloud Storage," in IEEE Systems Journal, vol. 17, no. 4, pp. 6334-6345, Dec. 2023, doi: 10.1109/JSYST.2023.3277194.

[25] Q. Xie, Z. Ding, W. Tang, D. He and X. Tan, "Provable Secure and Lightweight Blockchain-Based V2I Handover Authentication and V2V Broadcast Protocol for VANETs," in IEEE Transactions on Vehicular Technology, vol. 72, no. 12, pp. 15200-15212, Dec. 2023, doi: 10.1109/TVT.2023.3289175.

[26] A. Battah, K. Salah, R. Jayaraman, I. Yaqoob and A. Khalil, "Using Blockchain for Enabling Transparent, Traceable, and Trusted University Ranking Systems," in IEEE Access, vol. 11, pp. 23792-23807, 2023, doi: 10.1109/ACCESS.2023.3253948.

[27] Z. Guo, G. Wang, Y. Li, J. Ni, R. Du and M. Wang, "Accountable Attribute-Based Data-Sharing Scheme Based on Blockchain for Vehicular Ad Hoc Network," in IEEE Internet of Things Journal, vol. 10, no. 8, pp. 7011-7026, 15 April15, 2023, doi: 10.1109/JIOT.2022.3228550.

[28] C. Lin, X. Huang and D. He, "EBCPA: Efficient Blockchain-Based Conditional Privacy-Preserving Authentication for VANETs," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 3, pp. 1818-1832, 1 May-June 2023, doi: 10.1109/TDSC.2022.3164740.

[29] X. Wang, S. Garg, H. Lin, G. Kaddoum, J. Hu and M. M. Hassan, "Heterogeneous Blockchain and AI-Driven Hierarchical Trust Evaluation for 5G-Enabled Intelligent Transportation Systems," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 2, pp. 2074-2083, Feb. 2023, doi: 10.1109/TITS.2021.3129417.

[30] Y. Fu, S. Wang, Q. Zhang and D. Zhang, "Game Model of Optimal Quality Experience Strategy for Internet of Vehicles Bandwidth Service Based on DAG Blockchain," in IEEE Transactions on Vehicular Technology, vol. 72, no. 7, pp. 8898-8913, July 2023, doi: 10.1109/TVT.2023.3246221.

[31] K. Zhang, M. Deng, B. Gong, Y. Miao and J. Ning, "Privacy-Preserving Traceable Encrypted Traffic Inspection in Blockchain-Based Industrial IoT," in IEEE Internet of Things Journal, vol. 11, no. 2, pp. 3484-3496, 15 Jan.15, 2024, doi: 10.1109/JIOT.2023.3297601.

[32] S. Xu, X. Huang, J. Yuan, Y. Li and R. H. Deng, "Accountable and Fine-Grained Controllable Rewriting in Blockchains," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 101-116, 2023, doi: 10.1109/TIFS.2022.3217742.

[33] B. Jiang, Q. He, P. Liu, S. Maharjan and Y. Zhang, "Blockchain Empowered Secure Video Sharing With Access Control for Vehicular Edge Computing," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 9, pp. 9041-9054, Sept. 2023, doi: 10.1109/TITS.2023.3269058.

[34] Y. He, R. Jiang, X. Ni, S. Xu, T. Chen and J. Feng, "Blockchain-Based Access and Timeliness Control for Administrative Punishment Market Supervision," in IEEE Internet of Things Journal, vol. 10, no. 12, pp. 11054-11067, 15 June15, 2023, doi: 10.1109/JIOT.2023.3264805.

[35] Y. Xu, E. Yu, Y. Song, F. Tong, Q. Xiang and L. He, "$\mathcal {R}$-Tracing: Consortium Blockchain-Based Vehicle Reputation Management for Resistance to Malicious Attacks and Selfish Behaviors," in IEEE Transactions on Vehicular Technology, vol. 72, no. 6, pp. 7095-7110, June 2023, doi: 10.1109/TVT.2023.3238507.

[36] M. Salimibeni, Z. Hajiakhondi-Meybodi, A. Mohammadi and Y. Wang, "TB-ICT: A Trustworthy Blockchain-Enabled System for Indoor Contact Tracing in Epidemic Control," in IEEE Internet of Things Journal, vol. 10, no. 7, pp. 5992-6017, 1 April1, 2023, doi: 10.1109/JIOT.2022.3223329.

[37] Z. Wu, J. Liu, J. Wu, Z. Zheng and T. Chen, "TRacer: Scalable Graph-Based Transaction Tracing for Account-Based Blockchain Trading Systems," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2609-2621, 2023, doi: 10.1109/TIFS.2023.3266162.

[38] S. -C. Cha, C. -L. Chang, Y. Xiang, T. -J. Huang and K. -H. Yeh, "Enhancing OAuth With Blockchain Technologies for Data Portability," in IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 349-366, 1 Jan.-March 2023, doi: 10.1109/TCC.2021.3094846.

[39] M. Li, W. Wang and J. Zhang, "LB-Chain: Load-Balanced and Low-Latency Blockchain Sharding via Account Migration," in IEEE Transactions on Parallel

and Distributed Systems, vol. 34, no. 10, pp. 2797-2810, Oct. 2023, doi: 10.1109/TPDS.2023.3238343.

[40] D. A. Luong and J. H. Park, "Privacy-Preserving Identity Management System on Blockchain Using Zk-SNARK," in IEEE Access, vol. 11, pp. 1840-1853, 2023, doi: 10.1109/ACCESS.2022.3233828.

[41] K. Gai, S. Wang, H. Zhao, Y. She, Z. Zhang and L. Zhu, "Blockchain-Based Multisignature Lock for UAC in Metaverse," in IEEE Transactions on Computational Social Systems, vol. 10, no. 5, pp. 2201-2213, Oct. 2023, doi: 10.1109/TCSS.2022.3226717.

[42] P. Cao, G. Duan, J. Tu, Q. Jiang, X. Yang and C. Li, "Blockchain-Based Process Quality Data Sharing Platform for Aviation Suppliers," in IEEE Access, vol. 11, pp. 19007-19023, 2023, doi: 10.1109/ACCESS.2023.3246984.

[43] Y. Tian, B. Liu, Y. Li, P. Szalachowski and J. Zhou, "Accountable Fine-Grained Blockchain Rewriting in the Permissionless Setting," in IEEE Transactions on Information Forensics and Security, vol. 19, pp. 1756-1766, 2024, doi: 10.1109/TIFS.2023.3340917.

[44] M. Li, Y. Chen, C. Lal, M. Conti, M. Alazab and D. Hu, "Eunomia: Anonymous and Secure Vehicular Digital Forensics Based on Blockchain," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 1, pp. 225-241, 1 Jan.-Feb. 2023, doi: 10.1109/TDSC.2021.3130583.

[45] J. Ordóñez, A. Alexopoulos, K. Koutras, A. Kalogeras, K. Stefanidis and V. Martos, "Blockchain in Agriculture: A PESTELS Analysis," in IEEE Access, vol. 11, pp. 73647-73679, 2023, doi: 10.1109/ACCESS.2023.3295889.

[46] S. Xu, X. Huang, J. Yuan, Y. Li and R. H. Deng, "Accountable and Fine-Grained Controllable Rewriting in Blockchains," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 101-116, 2023, doi: 10.1109/TIFS.2022.3217742.

[47] H. Xie, J. Zheng, T. He, S. Wei, C. Shan and C. Hu, "B-UAVM: A Blockchain-Supported Secure Multi-UAV Task Management Scheme," in IEEE Internet of Things Journal, vol. 10, no. 24, pp. 21240-21253, 15 Dec.15, 2023, doi: 10.1109/JIOT.2023.3279923.

[48] Q. Zhuohao, M. Firdaus, S. Noh and K. -H. Rhee, "A Blockchain-Based Auditable Semi-Asynchronous Federated Learning for Heterogeneous Clients," in IEEE Access, vol. 11, pp. 133394-133412, 2023, doi: 10.1109/ACCESS.2023.3335603.

[49] Z. Wu, T. Shang, M. Yue and L. Liu, "ADS-Bchain: A Blockchain-Based Trusted Service Scheme for Automatic Dependent Surveillance Broadcast," in IEEE Transactions on Aerospace and Electronic Systems, vol. 59, no. 6, pp. 8535-8549, Dec. 2023, doi: 10.1109/TAES.2023.3306336.

[50] R. Shi et al., "Threshold Attribute-Based Credentials With Redactable Signature," in IEEE Transactions on Services Computing, vol. 16, no. 5, pp. 3751-3765, Sept.-Oct. 2023, doi: 10.1109/TSC.2023.3280914.