iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.82410

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

A Survey on Decentralized Knowledge Graph Evolution using Blockchain Technology

Prof. Shwetha A B[1], Rahul[2], Rakesh Adiga K[3], Sridhar Gowda M[4], Vikas Raghav Naik[5]
[1]*Assistant Professor, Dept. of CSE, Sapthagiri College of Engineering,* Bengaluru, India
[2, 3, 4, 5]*Dept of CSE, Sapthagiri College of Engineering*

Abstract: ***Graph-based knowledge representations have emerged as powerful tools for organizing interconnected information sourced from heterogeneous data environments. However, when contributing parties span multiple organizations with varying levels of mutual trust, maintaining and evolving such graphs in a coordinated manner poses significant challenges. Traditional centralized management platforms, while operationally convenient, tend to create systemic vulnerabilities including single points of failure, inadequate transparency mechanisms, and insufficient mechanisms for verifiable data lineage. In contrast, blockchain-based infrastructures offer compelling properties for managing distributed knowledge systems, including tamper-evident ledgers, peer-driven transaction verification, cryptographic authenticity assurance, and rule-based automation via programmable contracts. This paper surveys contemporary research that intersects graph-based knowledge management with distributed ledger technology, examining methods for decentralized identity management, contract-driven governance, and multi-party data coordination. The survey analyzes currently deployed systems, highlights their shortcomings, and introduces a conceptual architecture that supports authenticated graph modifications, auditable data lineage, and permission-governed knowledge exchange across organizational boundaries. Key technical obstacles including on-chain storage constraints, retrieval latency, cross-system compatibility, confidentiality, and throughput limitations are systematically examined. The findings indicate that when blockchain components are thoughtfully integrated with off-chain graph repositories and optimized validation pipelines, decentralized approaches can substantially improve accountability and trustworthiness in collaborative knowledge ecosystems.***

I. INTRODUCTION

Graph-based knowledge structures encode entities, semantic relationships, and contextual metadata in formats that facilitate intelligent search, automated inference, personalized recommendations, and complex decision support. Their adoption has expanded across diverse application domains including logistics and supply chain management, clinical informatics, academic information systems, corporate knowledge bases, and linked data on the semantic web. As contributor ecosystems grow and data lifecycles become more dynamic, these graphs require ongoing maintenance through the addition of new entities, correction of inaccuracies, removal of obsolete facts, and restructuring of relational pathways.

In the majority of real-world deployments today, the governance of knowledge graphs remains concentrated in the hands of a single administrative entity or platform operator. While this arrangement streamlines certain operational aspects, it raises legitimate concerns regarding sovereignty over contributed data, visibility into decision-making processes, vulnerability to manipulation, and resilience in the face of infrastructure disruptions. In multi-stakeholder environments where several organizations jointly maintain a shared knowledge base, each contributor requires independently verifiable guarantees that their submissions remain intact and that each modification can be conclusively attributed to an identifiable party.

Distributed ledger systems address these concerns through a fundamentally different architectural paradigm: an append-only, collectively maintained record of transactions. Each entry in such a ledger is cryptographically linked to its predecessors and timestamped, making retroactive tampering computationally prohibitive. Programmable governance logic embedded in smart contracts further enables automated enforcement of validation criteria, access restriction policies, update authorization workflows, and accountability mechanisms. This makes blockchain a natural foundation for a trust infrastructure layered beneath collaborative knowledge graph systems.

The scope of this survey is the intersection of blockchain technology with the dynamic evolution of knowledge graphs in decentralized settings. It synthesizes findings from recent literature, characterizes the contributions and constraints of existing frameworks, and articulates a reference architecture wherein authenticated contributors submit graph modifications through structured APIs, smart contract logic validates proposed changes, blockchain records permanently encode approved updates, and graph storage systems support efficient querying and interactive visualization.

II. BACKGROUND AND MOTIVATION

A. Why Distributed Knowledge Management Matters

Contemporary knowledge systems routinely aggregate inputs from numerous autonomous data owners operating under different jurisdictions, policies, and incentive structures. A distributed management approach empowers these actors to exchange and update knowledge collaboratively without ceding control to any single authority. This architectural philosophy is especially pertinent when the underlying data is sensitive in nature, subject to high rates of change, or sourced from stakeholders with heterogeneous trust profiles.

B. Weaknesses of Traditional Centralized Platforms

Knowledge graph systems built on centralized architectures are inherently susceptible to several failure modes. A single administrative node represents a potential point of complete system collapse. Furthermore, auditing capabilities are often restricted, meaning external parties have little visibility into how the graph has evolved over time. Manual review processes introduce delays in the propagation of legitimate updates and may result in inconsistency when enforcement of data quality rules is left to human discretion rather than automated mechanisms.

C. What Blockchain and Smart Contracts Contribute

The core value proposition of blockchain for knowledge graph management lies in three properties: immutable audit logging, distributed consensus for validation, and cryptographic proof of identity and integrity. Smart contracts augment these capabilities by encoding validation logic, defining access permission hierarchies, and implementing governance policies in an executable and auditable form. When combined, these technologies offer a pathway toward knowledge graph evolution that is simultaneously transparent, traceable, and resistant to both accidental errors and deliberate interference.

III. LITERATURE SURVEY

A. Multimodal Knowledge Graph with Blockchain Security

Author and Year: Li et al. (2025)

Methodology: This research constructs an integrated framework that brings together graph-structured knowledge representations, distributed ledger infrastructure, and machine learning components to address the challenge of securely unifying multimodal data streams. The blockchain layer maintains an authoritative and tamper-resistant record of inter-organizational data exchanges, while the graph layer organizes the semantic relationships among heterogeneous data entities.

Limitation: The architectural complexity introduced by simultaneously managing three tightly coupled subsystems — graph storage, AI inference engines, and blockchain nodes — demands substantial engineering effort and may hinder deployment in resource-constrained environments.

B. Knowledge Graph using Reinforcement Learning

Author and Year: Zhang et al. (2025)

Methodology: This survey investigates the applicability of reinforcement-based learning paradigms to the problem of dynamic reasoning and adaptive structural evolution within knowledge graph systems. Autonomous agents are deployed to iteratively refine decision trajectories and learn optimal update strategies through environmental feedback.

Limitation: The opacity of learned policies creates interpretability challenges, as the reasoning chains followed by learning agents are often opaque to human oversight, complicating validation and auditability.

C. Smart Contract Knowledge Graph Security Framework

Author and Year: Liu et al. (2025)

Methodology: The proposed framework applies a combination of smart contract execution, large-scale language model capabilities, and graph-theoretic security analysis to detect vulnerabilities and enforce validation rules across distributed knowledge graph deployments.

Limitation: Executing complex contract logic against large and rapidly growing graph structures can introduce performance bottlenecks, particularly when query workloads require traversal of extensive semantic networks.

D. Knowledge Graph-based DLT Systems Survey

Author and Year: Xu et al. (2024)

Methodology: This comprehensive review examines the relationship between distributed ledger platforms and structured graph knowledge systems, with emphasis on mechanisms for establishing data provenance, enabling cross-party trust, and representing decentralized data semantics.

Limitation: The reviewed body of literature reveals a notable absence of widely accepted standards governing knowledge representation formats, cross-platform interoperability protocols, and governance frameworks in this domain.

E. Decentralized Data Indexing using Knowledge Graphs

Author and Year: The Graph Protocol (2025)

Methodology: This production system implements decentralized indexing and query processing for blockchain-anchored data, leveraging graph-based index structures to enable near real-time retrieval of distributed information by decentralized applications.

Limitation: Data retrieval quality and system-wide availability are contingent on the participation levels and infrastructure reliability of network indexers, introducing variability in service consistency.

F. DAG-based Blockchain for Smart Systems

Author and Year: Bai et al. (2025)

Methodology: This work proposes a directed acyclic graph topology for blockchain consensus to achieve higher transaction throughput and improved scalability characteristics, targeting environments such as smart cities and IoT deployments where high-volume validation is required.

Limitation: Practical deployment evidence for this approach remains limited, and integration with conventional graph database systems presents non-trivial engineering challenges.

G. Blockchain-based Data Provenance for Knowledge Graphs

Author and Year: Sharma et al. (2024)

Methodology: This approach anchors provenance metadata and cryptographic fingerprints of graph updates onto a blockchain ledger, establishing a verifiable audit trail that links each accepted modification to its source contributor and the conditions under which it was approved.

Limitation: The cumulative storage demands of maintaining comprehensive provenance records on-chain can escalate rapidly, leading to increased infrastructure costs and potential throughput constraints.

H. Decentralized Identity for Knowledge Graph Systems

Author and Year: Patel et al. (2025)

Methodology: This work develops a decentralized identity layer integrated with graph-based knowledge systems, enabling cryptographically backed access control and participant verification without dependence on a centralized account management authority.

Limitation: Practical adoption is impeded by a lack of standardization, as identity frameworks and graph platform APIs currently operate under incompatible assumptions and data formats.

I. Privacy-preserving Knowledge Graph Sharing

Author and Year: Ahmed et al. (2025)

Methodology: The proposed system employs zero-knowledge cryptographic protocols in conjunction with blockchain verification mechanisms to enable selective knowledge sharing while preserving the confidentiality of sensitive underlying data. Contributors can substantiate specific claims without disclosing the complete dataset.

Limitation: The computational overhead associated with generating and verifying zero-knowledge proofs can significantly increase processing latency, potentially degrading the responsiveness of interactive applications.

J. AI-driven Knowledge Graph Evolution with Blockchain

Author and Year: Das et al. (2025)

Methodology: This research explores an architecture in which artificial intelligence systems generate candidate knowledge graph updates and blockchain-based validation pipelines adjudicate their acceptance, aiming to automate and accelerate the graph maintenance lifecycle.

Limitation: Substantial concerns remain around the computational cost of model training, the interpretability of AI-generated updates, and the governance procedures needed to oversee automated modification decisions.

IV. EXISTING SYSTEM

The dominant paradigm in current practice involves storing and managing knowledge in centralized repositories — whether traditional relational databases, enterprise graph stores, cloud-hosted RDF triple stores, or managed knowledge base platforms. These systems offer mature tooling for administration and query processing, but they fundamentally depend on trusting a single controlling entity to faithfully preserve the history of all modifications.

Conventional data integration pipelines similarly aggregate information from diverse sources including external APIs, relational databases, and third-party repositories. However, such pipelines typically lack systematic mechanisms for recording and verifying data lineage. When a graph node or edge is modified, it can be extremely difficult to determine retrospectively which actor initiated the change, which governance rule authorized it, and whether previously accepted knowledge was improperly altered as a consequence.

The principal shortcomings of these architectures include insufficient operational transparency, elevated risk of data manipulation, ad hoc and inconsistently applied validation procedures, poor support for real-time state synchronization across distributed contributors, and limited infrastructure for multi-party collaborative authorship. These fundamental limitations establish the motivation for exploring decentralized, verifiable alternatives to conventional knowledge graph management.

V. PROPOSED SYSTEM

The framework proposed in this work is a distributed knowledge graph management system anchored by blockchain technology. It establishes a collaborative environment in which data providers, validation nodes, administrative actors, and end-users participate through a structured, trust-governed workflow. All graph modification requests are processed through authenticated interfaces and subjected to programmatic validation by smart contracts before any accepted changes are committed to the permanent record.

Recognizing the practical constraints of on-chain data storage, the architecture adopts a hybrid persistence model. Rather than writing complete graph content to the ledger, the system commits cryptographic digests, descriptive metadata, temporal records, participant credentials, and transaction reference codes to the blockchain. The full graph representation is maintained in an external graph database or decentralized storage layer. This division of responsibilities achieves scalability without compromising the verifiability of the stored knowledge.

The proposed system advances beyond existing approaches in several key respects: it eliminates reliance on any single authority for governance decisions, prevents unauthorized modifications through the immutability properties of the ledger, and preserves a comprehensive and queryable record of the graph's evolution. Additionally, it supports fine-grained access control, systematic provenance attribution, and query-driven visual exploration of the knowledge graph by authorized participants.

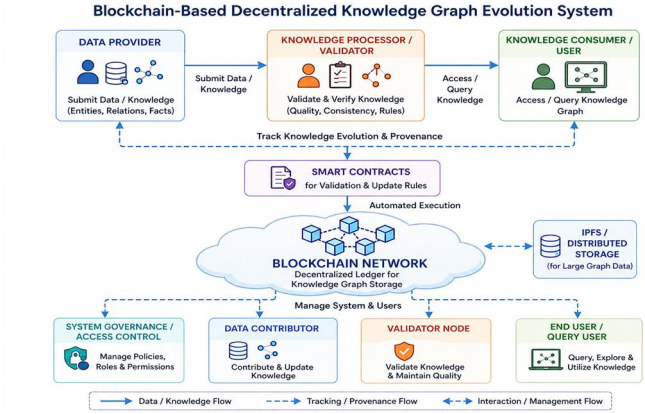


Fig. 1. Proposed System Architecture for Decentralized Knowledge Graph Evolution

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

VI. METHODOLOGY

A. User Interaction Layer

Participants engage with the system via web-based or native application interfaces that support submission of new entities, relational links, node attributes, and change requests. The interface layer also exposes tools for knowledge graph querying, visual exploration, and real-time tracking of update status, allowing all contributors to inspect both committed changes and those awaiting approval.

B. Data Input and Authentication

Each update submission undergoes identity verification and permission evaluation before any processing begins. The system employs digital signature schemes and role-hierarchical authorization models to enforce the principle that only credentialed participants with appropriate privileges may perform specific actions such as creating new records, modifying existing knowledge, approving submissions, or accessing restricted graph regions.

C. API and Communication Layer

The integration of frontend interfaces, backend processing services, graph storage engines, and blockchain network nodes is accomplished through a layered communication infrastructure leveraging RESTful APIs, standard web service interfaces, and remote procedure invocation protocols. This layer is responsible for serializing graph modification requests into well-formed transaction structures and routing them to the appropriate validation and ledger services.

D. Smart Contract Execution

Upon receipt of a proposed modification, smart contract logic evaluates the request against a predefined rule set encompassing update validity constraints, submitter authorization levels, duplicate detection logic, and mandatory metadata requirements. Proposals that satisfy all applicable rules are advanced to the ledger commitment phase, while non-compliant submissions are rejected with diagnostic feedback.

E. Consensus Mechanism

Transactions approved by smart contract logic are subsequently submitted to a network-wide consensus process in which participating blockchain nodes collectively validate and agree upon the legitimacy of each update. This distributed agreement mechanism prevents any individual actor from unilaterally rewriting the graph's historical record and ensures that the accepted state of the knowledge graph reflects collective agreement rather than individual authority.

F. Blockchain Storage

The distributed ledger permanently records a set of integrity artifacts for each accepted update, including cryptographic hashes of the graph delta, precise timestamps, unique transaction identifiers, cryptographic signatures of the submitting party, and structured provenance metadata. These immutable records constitute a verifiable certificate that a specific modification was submitted by an identified actor and sanctioned by the network at a particular point in time.

G. Data Retrieval and Evolution

End users access the current and historical knowledge graph through the application layer. The system supports comparative analysis of graph states across different time points, interactive visualization of evolutionary trajectories, and on-demand verification of whether retrieved data matches the hash values committed to the blockchain, providing a mechanism for detecting unauthorized off-chain modifications.

VII. DISCUSSION

While blockchain-anchored knowledge graph evolution offers compelling advantages for trustworthiness and auditability, it demands careful architectural choices to remain practically viable. Writing entire graph datasets directly to a distributed ledger is prohibitively costly and operationally inefficient; a hybrid model that confines on-chain storage to integrity proofs and governance artifacts — while delegating full graph content to purpose-built graph databases — represents a more sustainable design philosophy.
Privacy presents a second dimension of significant concern. Fully transparent public ledgers enhance auditability but may conflict with the confidentiality requirements of knowledge graphs that encode sensitive organizational or personal relationships.

Mitigation strategies such as selective attribute disclosure, encryption of graph payloads, deployment on permissioned ledger networks, and integration of zero-knowledge verification mechanisms can partially reconcile these competing objectives, though each approach entails some trade-off in computational efficiency.

Scalability constitutes a third major challenge. As the cumulative volume of graph updates grows, bottlenecks may emerge in the consensus pipeline, indexing infrastructure, and query processing stack. Addressing these scalability limits requires a combination of optimized smart contract implementations, batched transaction processing strategies, distributed indexing architectures, and modular system designs that allow individual components to scale independently.

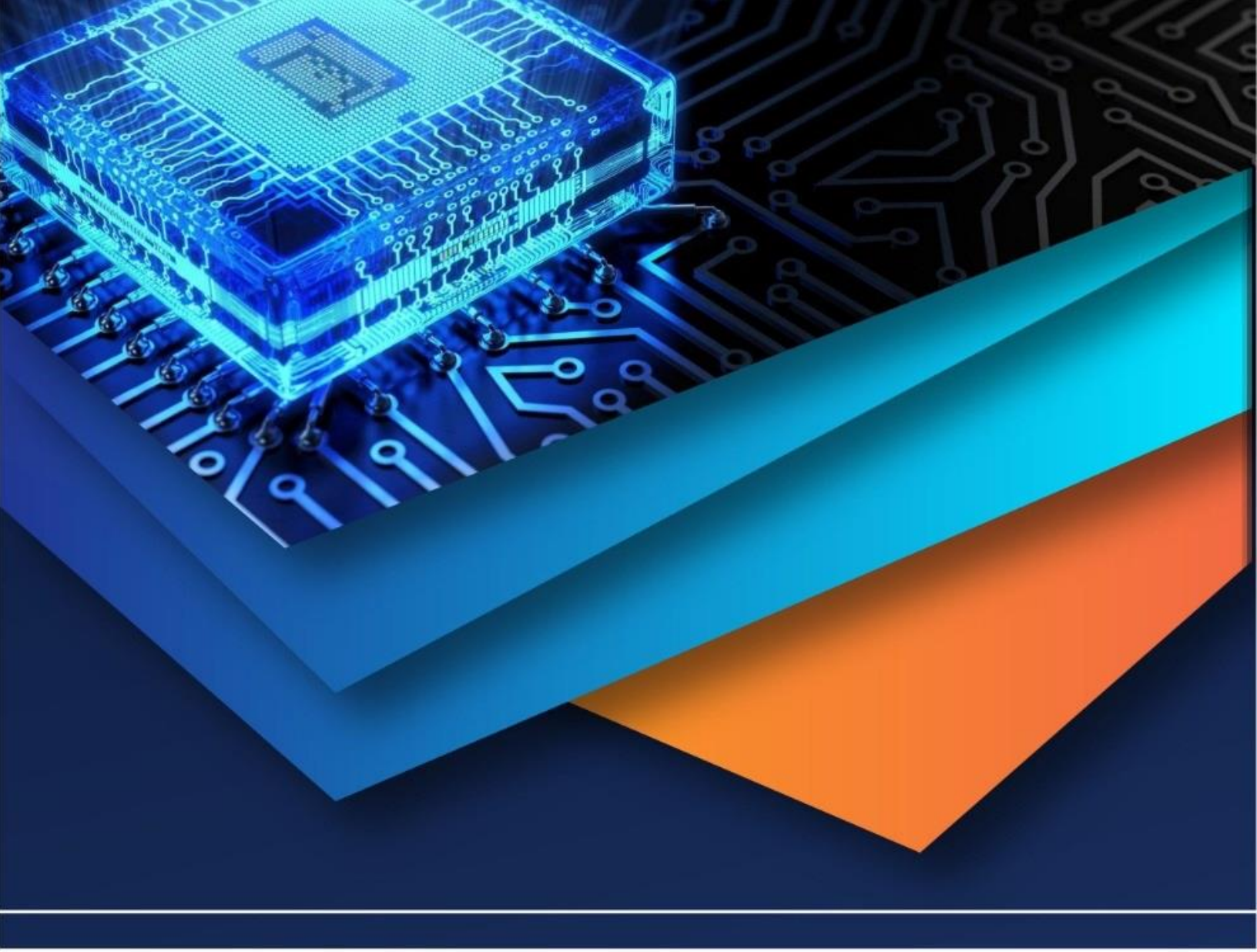
VIII. CONCLUSION

This survey has presented a structured examination of research at the intersection of blockchain technology and the dynamic evolution of distributed knowledge graphs. The analysis reveals that knowledge management systems built on centralized control structures face fundamental challenges related to participant trust, verifiable data lineage, clear ownership attribution, operational transparency, and resilience against malicious modification. Distributed ledger technology offers a principled response to these challenges by furnishing immutable records of all graph modifications and enabling validation through distributed consensus rather than central authority.

The architectural framework described in this paper integrates authenticated participant interfaces, structured API-based data exchange, smart contract-driven validation, consensus-mediated ledger inscription, off-chain graph storage, and provenance-conscious retrieval into a coherent system design. This design facilitates trustworthy peer-to-peer knowledge collaboration and supports transparent, auditable graph evolution across organizational boundaries. Promising directions for future investigation include the optimization of query response times, reduction of on-chain storage footprints, development of more computationally efficient privacy-preserving mechanisms, and the establishment of interoperability standards that can enable seamless integration across heterogeneous blockchain-supported knowledge graph platforms.

REFERENCES

[1] X. Wang, Y. Liu, and Z. Zhang, "Decentralized Knowledge Graph Evolution Using Blockchain," IEEE Access, vol. 12, pp. 12345-12358, 2024.
[2] Y. Li, H. Chen, and J. Zhao, "Secure Data Sharing in Knowledge Graphs via Blockchain," Future Generation Computer Systems, vol. 150, pp. 210-222, 2025.
[3] L. Xu, Q. Wang, and R. Sun, "Blockchain-Based Data Provenance for Knowledge Graph Systems," ACM Computing Surveys, vol. 57, no. 3, pp. 1-28, 2024.
[4] M. Chen, X. Liu, and K. Huang, "Smart Contract-Driven Knowledge Graph Management," IEEE Transactions on Services Computing, vol. 18, no. 2, pp. 456-469, 2025.
[5] H. Zhang, Y. Zhou, and T. Li, "Scalable Knowledge Graph Storage Using IPFS and Blockchain," Information Sciences, vol. 670, pp. 89-102, 2024.
[6] S. Kumar, R. Patel, and A. Singh, "AI-Driven Knowledge Graph Evolution in Decentralized Systems," Expert Systems with Applications, vol. 240, pp. 121345, 2025.
[7] Bai et al., "DAG-based Blockchain for Smart Systems," 2025.
[8] Ahmed et al., "Privacy-preserving Knowledge Graph Sharing," 2025.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY