International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Integration of Blockchain Technology in Database Management System (DBMS)

Mr. Wesley Wende[1], Mr. Promise Goodluck[2]

[1,2]Student, Computer Science, Sharda University

Abstract

This study explores integrating blockchain technology into traditional database systems to address data security concerns. By combining blockchain's immutability and decentralization with conventional databases, it aims to enhance data management system security. The study examines various implementation methods, including using blockchain as a layer, smart contract integration, and consensus mechanisms. Each approach's strengths and weaknesses are analyzed, providing insights into their potential applications. Key findings show that integrating blockchain significantly improves data security through enhanced traceability and tamper resistance. However, scalability and performance trade-offs are identified. This paper offers valuable insights for researchers and practitioners seeking innovative solutions for secure and reliable database systems.

Introduction

Blockchain, a distributed database, records transactions and events shared among participants. Verified by the majority, it's incorruptible due to its digital ledger and cryptographic hashes. Managed by a peer-to-peer network, it's a public ledger where nodes adhere to a consensus algorithm for adding and validating blocks. Blockchain's security and high fault tolerance make it a distributed computing system.

A database groups related data, while a DBMS organizes and manages it. DBMS minimizes redundancy, prevents inconsistencies, and provides features like concurrent access and backup. It efficiently stores and retrieves large amounts of data, allowing users to perform operations. Access control and transactions ensure data security.

Integrating blockchain into traditional DBMS creates hybrid databases. Blockchain's immutability prevents unauthorized modifications, while DBMS's efficiency optimizes performance. Combining these features creates a hybrid database with the best of both worlds.

Blockchain ensures data integrity by assigning unique hashes to each block.

Decentralized data management: Blockchain databases are stored on a network of computers. They're limited in scalability, have high costs, and are affected by regulations. However, they can be partially decentralized for critical transactions while keeping non-critical transactions centralized.

Smart contracts, computer programs that automate asset transfers based on conditions, integrate with traditional databases by bridging decentralized blockchain logic with centralized structured data storage. This integration enables data exchange and triggers smart contracts when specific database conditions are met, executing actions on the blockchain like transferring funds, updating records, or generating new transactions.

Objectives: Enhanced data security through blockchain technology.

Background: We'll overview traditional DBMS, including SQL vs. NoSQL. Key Differences between SQL and NoSQL

	ASPECT	SQL(relational)	NoSQL(non-relational)
1.	**Data Structure**	Table with rows and columns	Document-based, key value column-family, or graph-based
2.	**Schema**	Fixed schema (predefined structures)	Flexible schema(dynamic and adaptive)
3.	**Scalability**	Vertically scalable(upgrading hardware)	Horizontally Scalable(adding more servers)
4.	**Data integrity**	ACID-complaint(strong consistency)	BASE-complaint(more available, less complaint)
5.	**Query Language**	SQL(Structured Query Language)	Varies (e.g., MongoDB, uses its own query language)
6.	**Performance**	Efficient for complex queries and transactions	Better for large data and fast read/write operation
7.	**Use cases**	Best for transaction system(banking, ERP, etc)	Ideal for big data, real time web apps and data lakes
8.	**Example**	MySQL, PostgreSQL, Oracle, MS SQL servers	Mongo DB, Cassandra, CouchDB, Neo4j

In SQL, database are primarily called relational database (RDBMS) while NoSQL database are called non-relational or distributed databases. SQL is one of the most versatile and widely-used options available which makes it a safe choice for complex queries. SQL can also be restrictive as it requires the user to use predefined schemas to determine the structure of the data before the user can work with it. SQL databases can increase the load on a single server by increasing things like RAM, CPU or SSD. NoSQL databases on the other hand can handle more traffic by sharing, or adding more servers in NoSQL database. NoSQL can ultimately become larger and more powerful, making these database the preferred choice for large or ever-changing data sets. SQL follows the ACID properties (Atomicity, Consistency, Isolation and Durability) while NoSQL database follows the brewer CAP theorem (Consistency, Availability, and Partition Tolerance).

Key concept in Blockchain technology:

Distributed ledger

Distributed ledger Technology (DLT) is the technological infrastructure and protocol that allow simultaneous access, validation, and record updating across a network database. DLT is an important part of Blockchain Technology as it was created from it. The Infrastructure allows user view any changes and also view who in the network made the changes, this reduces the constant need to audit data and it ensures data is reliable. DLT enhances accountability, security and accessibility, it is still complex and difficult to scale.

DLT allows information to be stored securely and accurately using cryptography. The stored data can be accessed using "keys" and cryptographic signatures. Once the data is stored, it can become an immutable

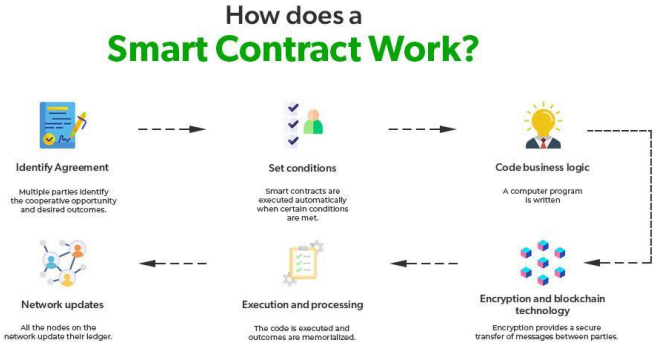
database. Due to the decentralized, private, encrypted nature, the distributed ledgers are less prone to cyber-attacks as the copies are stored across the network.

Some use cases of DLT include:
Secure, transparent, and decentralized transactions without a central authority.
Secure and tamper-proof digital identities to prevent identity theft.
Self-executing programs based on predefined conditions called smart contracts.
Blockchain consensus mechanisms are algorithms that blockchain network use to keep the network secure and operate smoothly.
There are many consensus mechanisms available, some of them are:
Proof of Stake (PoS): Validators stake tokens to become nodes and validate transactions, keeping the network secure. It requires less hardware and allows more participation.
Proof of Work (PoW): Validators solve complex puzzles to earn rewards. It's the first consensus mechanism for blockchain technology and is considered the most secure, reliable, and decentralized.
Proof of Authority (PoA) selects authorized transaction verifiers, such as VeChain's Masternode Operators, to validate transactions efficiently.
Proof of Activity (PoA): Combines Proof-of-Work (PoW) and Proof-of-Stake (PoS) for security and energy efficiency.
Proof of Identity (PoI) is a permissionless blockchain that grants voting power and rewards based on unique individual identity, potentially enabling universal basic income.
Proof of Elapsed Time (PoET) assigns blocks to validators based on a random waiting time, reducing energy consumption compared to Proof of Work blockchains.

Smart Contracts:
A smart contract is a computer program that automatically controls the transfer of digital assets between parties under specific conditions. It functions like a traditional contract but enforces it through code. Smart contracts execute as programmed, similar to traditional contracts enforced by law.

Features of smart contract:
Smart contracts are distributed, immutable, autonomous, transparent, and self-verifying. They are stored in a public blockchain and executed by all nodes.

Working of Smart Contract:
Smart contracts automate agreements by coding business logic and executing when conditions are met. Encryption and blockchain technology ensure secure authentication and verification, with outcomes recorded immutably.



Types of smart contract

Decentralized Autonomous Organizations DAOs are blockchain-based organizations governed by smart contracts, lacking centralized leadership. VitaDAO is an example of a DAO powering a scientific inquiry

Application Logic Contracts (ALCs) enable device-to-device interactions, such as blockchain integration and the Internet of Things.

Cryptographic Security in blockchain

Cryptography and hashing are fundamental concepts in blockchain, protecting transactions and ensuring data consistency. Cryptographic hashing, with its immutability and keyless nature, links blocks and maintains data integrity through unique hashes.

Cryptographic hash properties include immutability, sensitivity to data changes, and resistance to input guessing.

Cryptography in blockchain ensures secure data linking, prevents tampering, and enables irreversible transactions through encryption, digital signatures, and hash functions.

Cryptography in blockchain faces limitations, including difficulty accessing encrypted information, network attacks, and the need for additional methods to ensure high availability. It also doesn't protect against vulnerabilities from poor design and requires significant time and money investments.

Differences between centralized DBMS and decentralized blockchain systems.

Database	Blockchain
Database uses centralized storage of data.	Blockchain uses decentralized storage of data.
Database needs a Database admin or Database administrator to manage the stored data.	There is no administrator in Blockchain.
Modifying data requires permission from database admin.	Modifying data does not require permission. Users have a copy of data and by modifying the copies does not affect the master copy of the data as Blockchain is irresistible to modification of data.
Centralized databases keep information that is up-to-date at a particular moment	Blockchain keeps the present information as well as the past information that has been stored before.
Centralized databases are used as databases for a really long time and have a good performance record, but are slow for ertain functionalities.	Blockchain is ideal for transaction platform but it slows down when used as databases, specially with large collection of data.
Data can be easily deleted or modified if needed with proper authorization.	Data once entered cannot be deleted and is permanent in nature.
Cost-effective for most business applications as it requires less computational power.	More expensive to maintain due to high computational power requirements for consensus mechanisms.
Offers faster query and search capabilities for complex data structures.	Search and query operations are generally slower due to its distributed nature.
Vulnerability to single point of failure as data is stored in one central location.	Highly resistant to system failure due to distributed nature and multiple copies of data.
Real-time data processing and updates are more efficient.	Has inherent latency due to consensus mechanisms and block creation time.

Focus point in literature Review

Security Enhancements

Security is crucial in blockchain-integrated DBMS literature, as traditional databases face issues like unauthorized access, data tampering, and insider threats. Blockchain improves security through:

Decentralization: Distributing data across multiple nodes reduces the risk of single points of failure.

Immutability: Transactions can't be altered or deleted, ensuring historical integrity.

Access Control: Multi-signature authentication and decentralized identity solutions enhance access security.

Tamper-proof Storage: Altering data requires altering subsequent blocks, making tampering computationally infeasible.

How Blockchain Improves Data Integrity, Immutability, and Auditability in DBMS

Blockchain enhances traditional DBMS in three key aspects:

Data Integrity: Blockchain ensures accurate and consistent data across nodes through consensus mechanisms, reducing fraudulent activities.

Immutability: Unlike conventional databases, blockchain prevents retroactive alterations, crucial in sectors like finance and healthcare for accurate transaction histories.

Auditability: Blockchain maintains a transparent ledger of all transactions, enabling easy tracking and verification, beneficial for regulatory compliance and forensic investigations.

Cryptographic Techniques Used in Blockchain

Blockchain uses cryptography to secure transactions and maintain data integrity.

Hashing converts input data into a fixed-length string (hash) to ensure data integrity and prevent unauthorized modifications.

Public-key cryptography (e.g., RSA, ECC) encrypts data so only the intended recipient can decrypt it.

Digital signatures verify transaction authenticity using asymmetric cryptography (e.g., ECDSA).

Zero-Knowledge Proofs (ZKPs) allow one party to prove a statement's truth without revealing additional information.

Data Consistency & Performance

Traditional DBMS prioritize consistency, but blockchain's decentralized nature challenges immediate consistency. The literature highlights challenges like latency in blockchain networks, eventual consistency, and throughput limitations. Solutions include hybrid models, off-chain storage, and sharding to improve performance.

Scalability Issues

As blockchain adoption grows, scalability remains crucial. Traditional blockchain architectures struggle with large-scale DBMS applications due to low throughput, storage overhead, and high latency.

Solutions include layer-2 solutions like Lightning Network and Rollups, parallel processing with multiple chains or multi-threaded architectures, and consensus optimization with efficient mechanisms like Proof of Stake, Delegated Proof of Stake, or Directed Acyclic Graphs.

Interoperability

Interoperability refers to the ability of blockchain to integrate with traditional DBMS and other blockchains. Literature highlights several approaches:

Techniques for Integrating Blockchain with Traditional DBMS:

APIs: RESTful APIs and GraphQL interfaces enable blockchain data retrieval and interaction with conventional databases.

Middleware Solutions: Platforms like Oracle Blockchain Cloud Service facilitate data exchange between blockchain and traditional systems.

Interoperability Frameworks: Projects like Polkadot, Cosmos, and Chainlink enable communication between different blockchain networks and existing enterprise databases.

Use Cases

Blockchain's integration with DBMS is applied across various industries, each benefiting from its security, transparency, and efficiency.

Healthcare: Secure patient records, prevent unauthorized modifications, and block counterfeit medicines using blockchain.

Finance: Fraud-resistant transactions, automated financial agreements, and smart contracts.

Supply Chain: Transparent tracking, reduce fraud, and inefficiencies. Decentralized supplier management for quality standards.

Identity Management: Self-sovereign identity (SSI) for individuals to control their credentials, and blockchain-based authentication

.

Case Studies of Existing Blockchain-DBMS Integration:

IBM Food Trust: Uses blockchain to improve traceability in food supply chains.

Estonian Government's e-Health System: Uses blockchain for secure medical records.

JP Morgan's Quorum: A permissioned blockchain enhancing financial data security and privacy

Comparative Analysis of Blockchain and DBMS Integration Approaches

The integration of blockchain with traditional Database Management Systems (DBMS) is an emerging research area that aims to combine the security and transparency of blockchain with the efficiency and scalability of DBMS. Various approaches have been proposed, each with its own benefits and trade-offs.

Approaches to Blockchain-DBMS Integration

Relational DBMS and Blockchain Combination

Schuhknecht and Jörz (2022) explored integrating relational databases with blockchain using the Tendermint Core framework. This allows relational databases to execute deterministic SQL queries while maintaining blockchain's tamper-proof integrity. The study highlighted performance trade-offs, including throughput and latency overhead (Schuhknecht & Jörz, 2022).

Lightweight Blockchain Layer for Existing DBMS

Schuhknecht et al. (2021) proposed "chainify DB," a lightweight blockchain layer that sits on top of existing DBMS infrastructure. Their approach minimizes integration complexity while achieving up to 6x higher throughput compared to hyper ledger Fabric. However, there is still a small performance overhead of up to 8.5% (Schuhknecht et al., 2021).

Blockchain as a Standalone DBMS Alternative

The DBL (Deniable Blockchain Ledger) approach allows selective redaction of blockchain data while maintaining overall integrity using Chameleon Hash functions. This method enhances privacy and security but deviates from traditional DBMS functions (Chen & Chi, 2019).

Hybrid Blockchain and IoT-DBMS Systems

Several studies have investigated blockchain integration with IoT-based databases. Parmar and Shah (2023) emphasized secure data communication in IoT-DBMS environments using blockchain, focusing on authentication, access control, and data integrity (Parmar & Shah, 2023).

Blockchain in Micro service Architectures

Trebbau et al. (2021) presented a model-driven engineering approach for integrating blockchain into Microservice Architecture (MSA). Their method optimizes trust and authentication mechanisms but is more applicable for distributed, cloud-based applications rather than traditional DBMS (Trebbau et al., 2021).

Strengths and Weaknesses of Different Blockchain-DBMS Integration Models

Blockchain-DBMS integration models aim to balance decentralization, security, performance, and scalability. Here's an analysis of their strengths and weaknesses based on current research.

Relational DBMS with Blockchain (Tendermint Core-based Integration)

Example: Tendermint Core framework with relational DBMS (Schuhknecht & Jörz, 2022).

Strengths: SQL functionality with blockchain security, deterministic transactions, and permissioned/public setups.

Weaknesses: Lightweight blockchain layer on existing DBMS (chainifyDB) introduces performance bottlenecks and requires additional consensus mechanisms.

Strengths: Blockchain benefits without replacing existing DBMS, reducing complexity and overhead.

Weaknesses: Blockchain as a standalone DBMS alternative, such as the DBL approach, incurs an 8.5% performance overhead and may not fully replace DBMS security and transaction management.

Strengths: Enhances privacy, ensures data integrity, and eliminates centralized DBMS reliance.

Weaknesses: Blockchain redundancy hinders scalability and query efficiency..

Hybrid IoT-DBMS-Blockchain Integration

Example: IoT-blockchain integration for data security (Parmar & Shah, 2023).

Strengths: Enhances authentication, access control, and data integrity in IoT-DBMS transactions.

Weaknesses: Blockchain in microservices for authentication, as proposed by Trebbau et al. (2021), addresses high resource consumption and security complexity in IoT scalability.

Strengths: Enhances trust and authentication in distributed applications..

Weaknesses: Blockchain integration with traditional DBMS architectures requires significant redesign and offers trade-offs between security, scalability, and efficiency. The best choice depends on the specific use case.

Framework:

Deep Blockchain Framework (DBF)

Designed for security-based distributed intrusion detection and privacy-based blockchain with smart contracts in IoT networks.

Utilizes Bidirectional Long Short-Term Memory (BiLSTM) deep learning algorithm for intrusion detection.
Implemented using Ethereum library for privacy preservation (Al-Kadi et al., 2021).

Hammer: A General Blockchain Evaluation Framework

Provides systematic blockchain evaluation through workload prediction and asynchronous task processing.
Focuses on improving accuracy in evaluating blockchain performance (Wang et al., 2024).

Architecture Framework for Blockchain Implementation

Derived from design science research methodology with industry input.
Includes viewpoints such as applicability, ecosystem, infrastructure, legal considerations, and end-user experience (Lissåker & Sjöberg, 2019).

Neo Blockchain Actor Model Framework

Uses the Akka.NET framework to implement delegated Byzantine Fault Tolerance (dBFT) for consensus.
Focuses on scalability, reducing locks, and improving parallel execution (Suliyanti et al., 2021).

Blockchain Framework for Smart Mobility

Designed for secure data sharing in mobility networks.
Uses encrypted data storage, smart contracts, and decentralized control (López & Farooq, 2018).

Relational Blockchain Framework (Tendermint + Relational DBMSs)

Combines the Tendermint blockchain framework with relational DBMSs to achieve deterministic SQL execution.
Aims to balance blockchain features with database transaction processing (Schuhknecht & Jörz, 2022).

Algorithms:

Delegated Byzantine Fault Tolerance (dBFT) with Actor Model

Implements consensus via the Akka.NET framework to reduce deadlocks and improve scalability (Suliyanti et al., 2021).

Deniable Blockchain Ledger (DBL)

Introduces deniability by allowing transactions to be replaced with fake blocks while preserving blockchain integrity.
Uses Chameleon Hash functions for redaction (Chen & Chi, 2019).

Blockchain Governance Framework

Proposes a governance structure based on decentralization, incentives, decision rights, and accountability.
Addresses regulatory and ethical considerations (Liu et al., 2021).

Evaluation of Private Blockchain Frameworks (Parity vs. Multichain)

Analyses transaction validation time, mining time, and scalability.
Compares frameworks for optimal private blockchain implementation (Oliveira et al., 2019).

Challenges and Open Issues

Computational Overhead and Storage Requirements

Advancements in technology, particularly AI, blockchain, and big data analytics, increase computational and storage demands, posing challenges in scalability, cost, and efficiency. These challenges include high processing demands, storage scalability, energy consumption, and latency optimization.

Regulatory and Legal Concerns

Data Privacy and Security: Organizations must comply with regulations like GDPR, CCPA, and HIPAA by implementing secure data handling, anonymization, and encryption.

Technological Challenges: Cloud computing and blockchain operate across borders, creating jurisdictional challenges and legal ambiguity.

AI and Ethical Responsibility: AI-driven decision-making raises concerns about bias, transparency, and accountability, particularly regarding responsibility for incorrect or unethical decisions.

User Adoption and Industry Acceptance

Factors Influencing Technology Adoption: Resistance to change, usability, interoperability, trust and security, and economic considerations.

Challenges to Adoption: High switching costs, steep learning curves, lack of standardization, cybersecurity concerns, and uncertain ROI.

Solutions for Adoption: Ongoing research, industry collaboration, regulatory adaptation, energy-efficient computing, legal frameworks, and user-centric design.

Conclusion and Future Directions

Summary of Key Findings from the Literature

Blockchain technology offers notable benefits such as enhanced security, improved data integrity, and greater transparency within distributed systems. These attributes make it particularly valuable for applications where trust and data immutability are critical. However, the literature also highlights key challenges, including computational overhead, increased latency, and scalability limitations, which can hinder its performance in high-demand or real-time environments. To address these issues, researchers have proposed hybrid solutions that integrate blockchain with traditional Database Management Systems (DBMS), aiming to combine the strengths of both—blockchain's security and DBMS's efficiency.

Looking ahead, future research should focus on refining these hybrid architectures to improve performance and interoperability. This includes developing more efficient consensus algorithms suited for hybrid systems, exploring sharding and Layer 2 scaling techniques, and implementing adaptive mechanisms for dynamic load balancing. Furthermore, comprehensive case studies and empirical evaluations are essential to assess the practicality and impact of such systems across various sectors, including healthcare, finance, and supply chain management.

Research Gaps and Potential Directions for Future Studies

Future Research Directions: Scalability, interoperability, privacy, energy efficiency, and real-world applications.

Technical Challenges: Improving transaction throughput, reducing latency, optimizing storage, and standardizing protocols.

Privacy and Security: Exploring zero-knowledge proofs, secure multi-party computation, and encryption methods for data privacy.

Final Thoughts on the Feasibility and Future of Blockchain-DBMS Integration

While blockchain-DBMS integration holds promise for enhancing security and data integrity, its practical adoption depends on overcoming challenges related to scalability, computational efficiency, and regulatory compliance. Ongoing advancements in blockchain protocols, hybrid architectures, and industry-specific use cases will determine its long-term viability. With further research and technological innovation, blockchain-DBMS integration could become a fundamental component of secure and

transparent data management in various industries, including finance, healthcare, and supply chain management.

References

1. Databases fit for blockchain technology: A complete overview
2. Blockchain technology can be enhanced by using different DBMS types, such as transactional, analytical, hybrid, and blockchain, to achieve high throughput, low latency, and Blockchain technology – recent research and future trend Blockchain technology is an emerging technology in its early development stage, with potential for future research directions in information systems.
3. A bibliometric analysis and visualization of blockchain Future blockchain research should focus on management, blockchain technology, energy, machine learning, and smart homes.
4. Incorporating blockchain technology in information systems research Blockchain technology is crucial for information systems research, and this special issue highlights the need for such research and highlights nine outstanding articles selected for publication.
5. A Systematic Literature Mapping on Using Blockchain Technology in Identity Management Blockchain-based identity management research mainly focuses on solutions and architectures, with no long-term collaboration and lack of real-world products.
6. Blockchain and supply chain management integration: a systematic review of the literature Blockchain-SCM integration is in its infancy, but smart contracts in the electric power industry show potential for disrupting traditional industries like healthcare, transportation, and retail.
7. Data-driven review of blockchain applications in supply chain management: key research themes and future directions Blockchain applications in supply chain management can improve revenue management, sustainability, traceability, and anti-counterfeit systems, with potential future directions including integration with emerging technologies and decentralized autonomous organizations.
8. Blockchain in the AECO industry: Current status, key topics, and future research agenda Blockchain research in the AECO industry focuses on contract management, supply chain management, information management, stakeholder management, and technology integration.
9. Where Is Current Research on Blockchain Technology?—A Systematic Review Current Blockchain research mainly focuses on Bitcoin and privacy, with less than 20% on other applications, and many solutions lack concrete evaluation and scalability challenges remain unstudied.
10. Blockchain in accounting practice and research: systematic literature review Blockchain technology has potential implications for accounting practices and research, including triple-entry bookkeeping, transaction inalterability, automation, and representation of cryptocurrencies in financial statements.
11. Blockchain in Enterprise Resource Planning Systems: A Comprehensive Review of Emerging Trends, Challenges, and Future Perspectives
12. Blockchain integration in ERP systems shows promise for enhanced security, transparency, and efficiency, but faces technical and organizational challenges.
13. Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions IoT and blockchain integration has the potential to transform supply chains and secure healthcare data, with 14 distinct research themes identified using Latent Dirichlet Allocation.
14. Blockchain Propels Tourism Industry - An Attempt to Explore Topics and Information in Smart Tourism Management through Text Mining and Machine Learning Blockchain technology has the

potential to revolutionize the tourism industry by enhancing hospitality, accommodation, and booking processes.

15. Integrating blockchain with building information modelling (BIM): a systematic review based on a sociotechnical system perspective Blockchain integration in BIM has potential for security, traceability, and transparency in the construction industry, but significant gaps remain between potentials and widespread adoption.