iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.69805

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 13 Issue IV Apr 2025- Available at www.ijraset.com

Blockchain Based Data Sharing System

Gaurav Kumar[1], Gulfam Khan[2], Kamran Khan[3], Anmol Mishra[4], Dr. Abdul Alim[5], Ms. Arti Attri[6], Dr. Sureshwati[7]
[1, 2, 3, 4]*Department of Computer Applications, Greater Noida Institute of Technology (Engg. Institute), Greater Noida, India*
[5, 6, 7]*Assistant Professor, Department of Computer Applications, Greater Noida Institute of Technology (Engg. Institute), Greater Noida, India*

Abstract: ***With the exponential increase of digital data, safe and efficient data sharing has become an important challenge. Traditional centralized systems face issues such as data violations, lack of transparency and single point of failure. Blockchain technology provides a decentralized, tampering-proof and transparent solution to share data in many stakeholders. This paper examines the architecture, benefits, challenges and potential applications of the blockchain-based data sharing system. We analyze various consensus mechanisms, smart contracts and cryptographic techniques that increase security and trust in the data exchange. Additionally, we discuss real -world implementation and future research directions in this domain.***
Keywords: Blockchain, Data Sharing, Decentralization, Smart Contracts, Security, Privacy.

I. INTRODUCTION

Data sharing is required in various fields including healthcare, finance, supply chain and IoT. However, traditional central systems suffer from weaknesses such as unauthorized access, data manipulation and privacy. Blockchain technology offers a promising settlement for a safe and transparent data sharing with its decentralized and irreplaceable account book. In today's digital age, data is new oil-a valuable resource that runs innovation, decision making and economic development. From healthcare records and financial transactions to chain logistics and Internet of Things (IOT) devices, large -scale data is generated and exchange of every second. However, as data sharing becomes more important, there are challenges associated with it. Traditional centralized systems, where a single unit controls data storage and access, is rapidly weakening for cyber-attacks, privacy violations and disabilities. Enter blockchain technology - a revolutionary approach to data sharing promises of safety, transparency and decentralization. Originally developed as a spine of cryptocurrency such as bitcoin, blockchain is safe and developed in a powerful tool for tampering-proof data exchange. Unlike the traditional database managed by a central authority, it distributes data to a network of blockchain nodes, ensuring that no point of failure exists. But why is there such a game-changer to share blockchain data? And what are the implications of the real world of adopting this technique? This paper examines these questions, which engage the blockchain-based data sharing system in mechanisms that make more secure, efficient and reliable than traditional models. Essentially a allotted ledger maintained across a peer-to-peer network. Unlike conventional databases, a blockchain is decentralized, which means that no single entity has entire manage over the records or the infrastructure. Blockchain, at first brought as the underlying era behind Bitcoin, is Each transaction is cryptographically secured, proven via consensus mechanisms, and recorded immutably on the ledger. This shape inherently promotes transparency, protection, and resistance to tampering, making it a possible foundation for constructing strong data sharing structures.

A. The Problem With Traditional Data Sharing Before

information how blockchain can remodel statistics sharing, it's vital to understand the limitations of current structures. Most organizations depend upon centralized databases, wherein a unmarried server or entity stores and controls access to data. While this model has labored for decades, it comes with good sized drawbacks:

1) Security Vulnerabilities

Centralized databases are high goals for hackers. A single breach can expose thousands and thousands of touchy records—think of incidents like the Equifax facts breach (2017), in which nonpublic information of 147 million human beings become stolen. Since all information is stored in a single area, attackers best want to compromise one machine to benefit get right of entry to.

2) Lack of Transparency & Trust

In many industries, stakeholders don't completely agree with every other with information. For instance:

- Healthcare: Hospitals and insurance groups regularly battle to share affected person records securely.

- Supply Chain: Manufacturers, suppliers, and shops might also manipulate data to cover inefficiencies or fraud.
- Finance: Banks and fee processors rely on intermediaries, growing costs and delays. Without a obvious machine, verifying the authenticity of shared data turns into tough

3) Single Point of Failure

If a primary server is going down (because of cyberattacks, technical screw ups, or natural screw ups), the complete information-sharing surroundings collapses. This creates bottlenecks and disrupts important operations.

4) Privacy Concerns

Many centralized platforms gather excessive consumer statistics, main to privacy violations. Regulations like GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act) impose strict regulations on information managing, but enforcing compliance stays difficult.

B. How To Solve These Challenges Blockchain

The blockchain introduces data sharing in a decentralized, tampering-proof and transparent manner. Here is how it addresses the shortcomings of traditional systems:

1) Decentralization

Not a single point of control Instead of storing data on a server, the blockchain distributes it to a network of computers (nodes). Each node account has a copy of the book, which means: No unit can manipulate data. The system still remains when some node fails. Users do not need to rely on a central authority - the trust is designed in technology.

2) Disqualification

Tamper-proof record Once the data is recorded on the blockchain, it cannot be converted or removed. Each transaction is cryptographically connected to the previous one, with many types of blocks. If someone tries to change the record, the entire network rejects modification. This makes the ideal for blockchain: Audit trails (eg, financial transactions monitor). Legal documents (eg, property records that should remain untouched). Medical history (eg, is not wrong to ensure the patient's records).

3) Smart Contracts

Automatic and Reliable Agreement Smart contracts are self-planned programs that run on blockchain. They automatically apply rules when they meet predefined conditions. For example: A healthcare smart contract can provide temporary access to the patient's record of the patient when the patient gets approval. A supply chain smart contract can release payment to a supplier when a shipment is verified by IOT sensor. This eliminates the requirement of middlemen, reduces costs and delays.

C. Publicity, Privacy, and Selective Data Sharing

Not all data needs to be made fully public. Blockchain allows for selective disclosure through various mechanisms:

- Permissioned Blockchain: Only authorized participants can access the data. This is commonly used in enterprise solutions such as *Hyperledger Fabric*.
- Zero-Knowledge Proofs (ZKPs): Users can prove possession of certain information (e.g., age or credit score) without revealing the actual data.
- Encrypted Data Storage: Sensitive information can be stored off-chain, with only verification hashes placed on the blockchain.

II. LITERATURE REVIEW

The safe and efficient sharing of data is important, especially with new technologies like cloud computing, the Internet of Things (IoT), and big data. These technologies usually store data in one main location, leading to trust, privacy, and security issues. Blockchain technology provides a fresh way to manage and share data. Instead of keeping all data in one place, it uses methods that spread out the data. These methods make sure data can't be changed and allow everyone to see what happens with the data. This approach is different from old data management methods.

The exponential boom of virtual records in current years has intensified the want for steady and transparent information sharing systems throughout multiple industries. Traditional facts sharing mechanisms are in most cases centralized, main to demanding situations which include statistics breaches, limited accept as true with among stakeholders, lack of transparency, and inadequate consumer manage. Blockchain technology has emerged as a transformative solution, providing decentralized and tamper-resistant information management that addresses a lot of these troubles.

Early research by way of Zyskind, Nathan, and Pentland (2015) laid the foundation for blockchainprimarily based private information management. Their paintings introduced the idea of using blockchain and smart contracts to give people control over how their personal information is shared. In this model, smart contracts permit computerized enforcement of get admission to permissions, ensuring that information is best handy beneath user-described situations.

Further tendencies have focused on the usage of blockchain in sensitive domain names which include healthcare. Azaria et al. (2016) added MedRec, a blockchain-primarily based device for coping with electronic scientific records. This machine emphasizes patient-centric manipulate, permitting stable and traceable get entry to to health statistics by using vendors and researchers whilst protective privateness. Similarly, Yue et al. (2016) proposed a hybrid method, wherein large scientific facts is stored off-chain even as metadata and get admission to permissions are managed on the blockchain.

Smart contracts play a critical function in automating information governance. Liu et al. (2020) explored their use in decentralized get admission to manage structures, permitting records owners to define, adjust, and revoke access rights without counting on centralized authorities. Attribute-Based

Encryption (ABE) and Role-Based Access Control (RBAC) models have also been integrated with blockchain, providing fine-grained control over data sharing. Liang et al. (2021) demonstrated that such models can enhance both security and flexibility in access management.

2022 tackled this by using anomaly detection and the Synthetic Minority Over-Sampling Techniques (SMOTE). These methods helped balance the datasets and made fraud detection more accurate. They also explored cost-sensitive learning, which aims to enhance fraud detection by imposing greater penalties for incorrectly identified fraud.

A. Challenges in Blockchain-Based Data Sharing Systems

Scalability Issue

- Limited transaction throughput (e.g., Bitcoin and Ethereum take care of just a few transactions according to second).
- Performance bottlenecks due to community consensus mechanisms.

High Energy Consumption

- Public blockchains (like Bitcoin) that use Proof of Work (PoW) require considerable computational electricity and strength.

Data privacy worry

- Public blockchains appear to all transaction data, which can highlight sensitive metadata.
- It is difficult to follow secrecy laws such as GDPR (eg, "right to forget").

Storage limits

- The blockchain is not designed to store large amounts of data.
- Off-chain storage (eg, IPF) adds complexity and introduces new security concerns.

Shortage of difference

- Various blockchain platforms have limited ability to communicate or share data with each other.
- No universal standard for cross-chain data exchange.

Smart Contract Vulnerabilities

- Bugs or flaws in clever contracts can lead to records leaks or unauthorized get entry to.
- Smart contracts are immutable once deployed, making fixes hard.

User Identity and Access Management

- Managing decentralized identity securely is hard.
- Ensuring proper authentication and authorization without compromising decentralization

Adoption barriers

- Lack of technical understanding and resistance to change from traditional systems
- The initial configuration costs and the complexity of integration can be high.

Governance Challenges

- Decentralized systems need consensus on change, which can be slow or politically difficult.
- Protocol or forks updates can fragment networks.

III. METHODOLOGY

The methodology of this take a look at is targeted on designing, growing, and studying a prototype blockchain-based information sharing system to illustrate how blockchain may be efficiently used to beautify the safety, transparency, and manipulate in records sharing environments. The technique consists of four primary stages: gadget design, era choice, prototype implementation, and assessment.

A. Requirements Analysis

Functional Requirements

- Secure authentication and get right of entry to control
- Immutable audit trails for records transactions
- Real-time information synchronization
- Interoperability with existing structures

Non-functional requirements

- Scalability to handle growing data volumes
- Less delayed transaction process
- Power efficiency
- Regulatory compliance (GDPR, HIPAA)

B. System Design

The design phase involves identifying the key requirements of a safe and decentralized data sharing platform. The system is architect with the following core components:

Blockchain Network: Metadata serves as an irreversible account book to store access logs and permissions.

Off-chain storage: Handles storage of large files to remove blockchain storage boundaries (eg, using IPF or cloud services).

Smart Contracts: Control the logic for access permissions, data requests and transaction handling.

C. Technology Stack Selection

To build and examine the prototype, suitable blockchain systems and tools were selected based totally on elements which include scalability, help for smart contracts, ease of improvement, and network assist:

- Blockchain Platform: Ethereum – chosen for its adulthood, smart settlement skills, and sturdy improvement tools.
- Smart Contract Language: Solidity – the primary language for Ethereum smart contracts.
- Data Storage: IPFS (Inter Planetary File System) – used for decentralized, off-chain storage of actual data and documents.
- Frontend: React.Js – for building the consumer interface for importing and inquiring for information.
- Wallet Integration: MetaMask – to allow users to signal transactions and engage with smart contracts.

D. Prototype Implementation

A Blockchain -based data sharing system operating prototype has been developed using the above technologies. The process includes:

Step 1: Data encryption and upload

- The user encrypts the file locally before sending it to IPFS.
- IPFS returns a hash (ICD) that identifies and locates the file exclusively.

Step 2: Metadata storage in blockchain

- The file's hash, owner ID and relevant metadata (eg upload time, description) are stored in the Ethereum blockchain through an intelligent contract.
- A file and property record is now unchanging.

Step 3: Access Permission Management

- The data owner uses an intelligent contract to grant rights of access to other users (public address).
- The intelligent contract updates permission mappings in the chain

Step 4: Data Access Request

- A user sends a request to access a specific file through the user interface.
- If the user has permission, the smart contract validates the request and provides access by returning the IPFS hash.

Step 5: Monitoring and Audit

- All actions (upload, permission grant, access request) are logged on-chain.
- A dashboard allows users to view their data transactions and access logs for transparency.

E. Evaluation Criteria

- Security: Ensures handiest legal customers can get right of entry to statistics; records are immutable.
- Transparency: All get right of entry to and sharing movements are logged and verifiable.
- User Control: Users can define, update, and revoke access to their information.
- Efficiency**:** Evaluated response time and throughput under simulated load.
- Scalability: Assessed the feasibility of large-scale deployment using test net simulations

IV. CONCLUSION

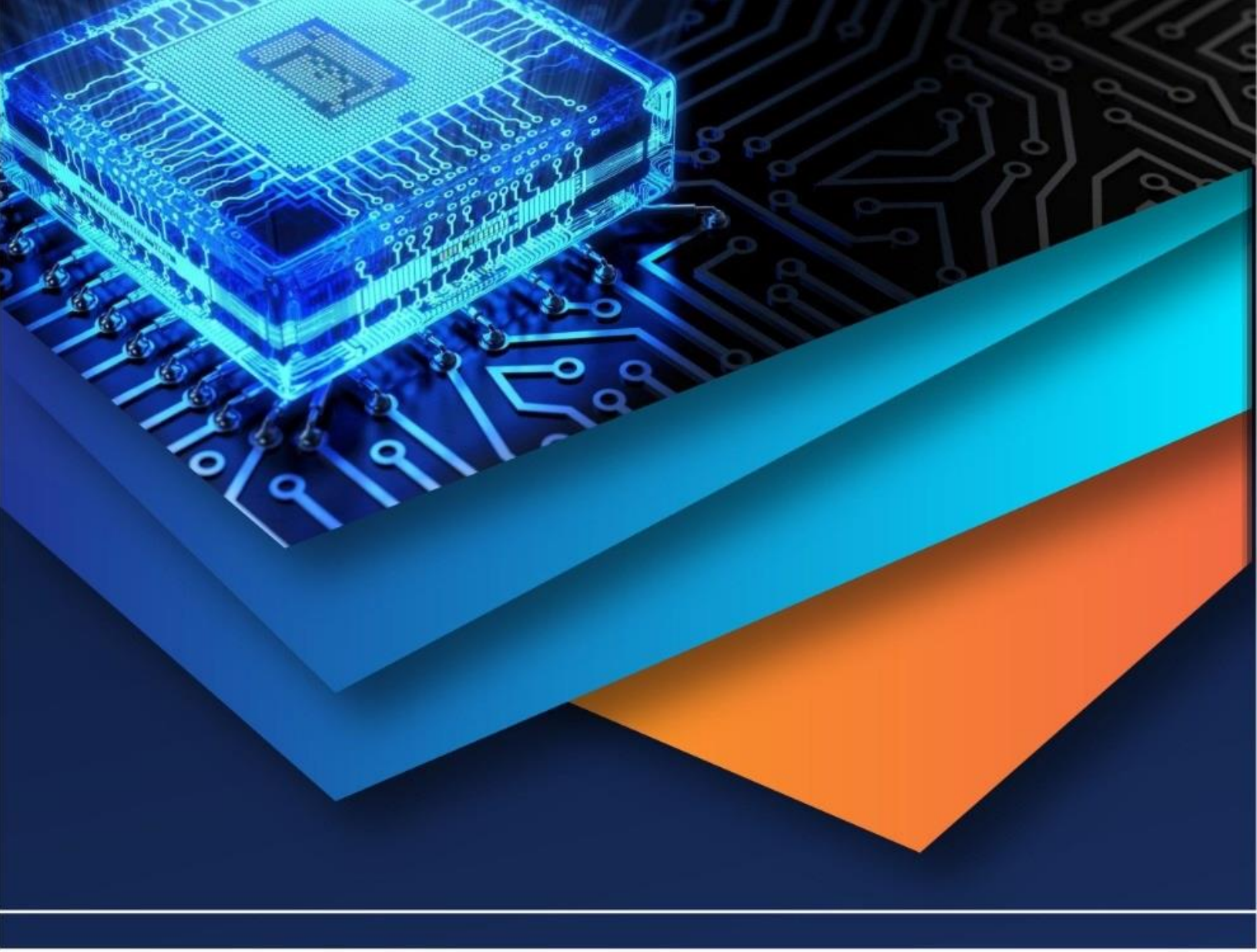
Blockchain based data sharing - systems provide a safe, transparent and efficient option for traditional centralized models. While challenges such as scalability and regulation persist, progress in consensus mechanisms and privacy-conservation techniques is paving the way for widespread adoption. Future research should focus on adaptation of performance and ensuring compliance with global data protection laws. In today's digital age, safe and efficient distribution of data for the operation and progress of numerous areas including healthcare, finance, supply chain, education and more is essential. Traditional data sharing systems, which depend very much on central architects, have shown more and more their limitations - especially in terms of breach of data, lack of transparency and inadequate user control. The emergence of blockchain technology gives a pattern of how the data can be operated and shared in a decentralized, secure and transparent way.

This article examined the core concepts, architecture and applications of blockchain-based data sharing systems. The basic strength of blockchain lies in it's can enforce granular access controls and automate permission management, and ensure that data is only divided under agreed conditions. ability to maintain an unchanging, distributed main book that provides verifiable and tamper fast records of all data transactions. By eliminating the need for centralized intermediaries, blockchain improves confidence among participants, even in environments where parties may not completely trust each other. Through the integration of smart contracts, computer owners

This paper explores these opportunities in depth, analyzing architectures, use cases, and emerging trends that will shape the future of data sharing.

REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf(Seminal paper introducing blockchain technology)
[2] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), pp. 352375. https://doi.org/10.1504/IJWGS.2018.095647
[3] IBM. (2020). IBM Food Trust: Blockchain for supply chain transparency. https://www.ibm.com/products/food-trust(Case study on blockchain in supply chains)
[4] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. 2nd International Conference on Open andBigData. https://doi.org/10.1109/OBD.2016.11
[5] (Blockchain in healthcare)
[6] Buterin, V. (2013). Ethereum white paper: A next-generation smart contract and decentralized application platform. https://ethereum.org/en/whitepaper/
[7] European Union. (2016). General Data Protection Regulation (GDPR). https://gdpr-info.eu/ (Legal challenges for blockchain immutability)
[8] Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media. (Book on broader blockchain applications)
[9] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. IEEE Security & Privacy, 15(4), 20-28. https://doi.org/10.1109/MSP.2018.3111245
[10] (Privacy solutions like zero-knowledge proofs) Hyperledger Foundation. (2022). Hyperledger Fabric documentation. https://hyperledgerfabric.readthedocs.io/ (Private/consortium blockchains)
[11] World Economic Forum. (2021). Blockchain for decentralized governance. https://www.weforum.org/reports/blockchain-decentralized-governance (Future trends and policy recommendations)
[12] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
[13] Hyperledger Foundation. (2023). Hyperledger Fabric Documentation.
[14] Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger.
[15] Zhang, Y., & Xue, R. (2018). "Security and privacy on blockchain." ACM Computing Surveys.
[16] Zyskind, G., Nathan, O., & Pentland, A. (2015). "Decentralizing privacy: Using blockchain



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY