Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 13s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Dynamic Access Control System Using Blockchain Technology and Provenance

Thippireddy Harika[1], Dr. Gera Pradeepini[2]

[1]Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Guntur, India
Email ID: thippireddyharika@gmail.com

[2]Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Guntur, India
Email ID: pradeepini_cse@kluniversity.in

Cite this paper as: Thippireddy Harika, Dr. Gera Pradeepini, (2025) Dynamic Access Control System Using Blockchain Technology and Provenance. *Journal of Neonatal Surgery*, 14 (13s), 83-92.

ABSTRACT

Blockchain technology has drawn a lot of interest because it can provide transparent, decentralized, and safe systems, which makes it a viable option for access control systems. Limitations with trust, scalability, and susceptibility to unwanted access are common with traditional centralized access control systems. Blockchain addresses these concerns providing secure, decentralized, and transparent systems, presenting a viable approach to access control systems. To get around the drawbacks of conventional systems, this research presents a revolutionary blockchain-based dynamic access control mechanism that takes provenance into account. The suggested architecture combines provenance with blockchain technology to produce a decentralized dynamic access control solution that can be tailored to different situations and access needs. The scheme allows dynamic updates to policies for access control, adjusting permissions based on changing conditions such as user roles, time, or context. This dynamic adaptability ensures that access privileges remain aligned with current needs, without requiring centralized intervention. It provides a robust, scalable approach for managing access control in environments where data integrity and accountability are critical Overall, by using a decentralized ledger to store access records, guaranteeing transparency and immutability, it provides a solid and scalable method for managing access control in settings where data integrity and accountability are crucial.

Keywords: *Blockchain Integration, Provenance Tracking, Dynamic Access Control, Smart Contract Enforcement, Decentralized Ledger.*

1. INTRODUCTION

In order to assure that only authorized people or entities can enter particular system coffers, access control techniques are required. Traditional approaches of access control [1] similar as part- Grounded Access Control or Discretionary Access Control (DAC), are generally employed in centralized systems where access opinions are made by a central authority. While these systems have served their purpose, they frequently face challenges [2], including scalability, single points of failure, and vulnerability to vicious interposers or unauthorized access. Likewise, centralized systems can struggle to acclimatize to evolving conditions, leading to inefficiencies and a lack of inflexibility.

The Importance of Dynamic and Flexible Access Control in Modern Applications Access control must be dynamic and flexible in contemporary operations, especially remote environments, pall computing, and the Internet of Things. Stationary programs are frequently inadequate to handle the complications of the real-time, environment-apprehensive access opinions. For illustration, access rights may change based on time, position, stoner places, or environmental conditions. A flexible access control system that can acclimate programs on- the cover is critical for meeting the demands of contemporary operations, ensuring that security and usability are maintained while accommodating dynamic surroundings. Blockchain technology has gained attention for its capability to give decentralized, transparent, and secure systems.

By storing data in a distributed tally, blockchain reduces the possibility of single points of failure, does away with the necessity for a central authority, and enhancing security. Blockchain provides a transparent and safe approach for monitoring data access and authorization by guaranteeing that access records are empirical and unchangeable. Blockchain's decentralized structure makes it the perfect solution for environments with high levels of responsibility, security, and trust.

Concept of Provenance and Its Significance in Ensuring Data Responsibility, Provenance refers to the shadowing of the origin and history of data, including who penetrated it, when, and why. Provenance mechanisms ensure that every action performed on data is traceable, furnishing a transparent inspection trail. This is pivotal for responsibility, as it enables the

verification of access opinions and ensures that any data manipulation is duly logged. Provenance not only, strengthens security but also supports compliance conditions and enhances trust in the system.

This research aims to transform traditional access control systems by introducing an innovative framework built on blockchain technology, complemented by provenance tracking. The primary objectives of this study are to significantly enhance the flexibility, security, and scalability of access control systems while ensuring the integrity and accountability of data through meticulous provenance monitoring.

Contributions of the Paper:

In this work, we propose a pioneering framework that effectively merges the principles of blockchain with provenance tracking to deliver dynamic, secure, and decentralized access control solutions. Our principal contributions include several key advancements:

1. Blockchain-Based Access Control System: We have developed an advanced access control framework rooted in blockchain technology. This system guarantees that all access requests and transactions are recorded on an immutable ledger, thereby enhancing the reliability and security of access permissions. Blockchain's decentralized structure reduces the possibility of unauthorised manipulation or breaches, establishing a strong foundation for trust within the system.

2. Implementation of Provenance Tracking: To facilitate comprehensive data traceability, we have integrated provenance tracking into our framework. This integration allows for thorough monitoring of the data lifecycle, including the identity of who accessed specific data, when access occurred, and the purpose behind it. By maintaining a detailed record of access events, we enhance accountability and empower organizations to effectively audit their access control policies.

3. Utilization of Smart Contracts: Our framework incorporates smart contracts to automate policy enforcement. These self-executing contracts enable real-time decision-making regarding access permissions based on predefined conditions. By automating access control processes, we reduce reliance on manual interventions, thereby increasing efficiency and facilitating a more responsive approach to changing access needs.

4. Enhanced Flexibility and Scalability: Through our innovative approach, the proposed system is designed to adapt to various organizational requirements. The combination of blockchain and provenance tracking allows for a flexible policy framework that can be readily updated in response to evolving security demands or operational changes. Additionally, the decentralized architecture supports scalability, enabling organizations to manage growing user bases and increasing volumes of data without compromising security.

5. Greater Accountability: Our groundbreaking framework not only enhances operational efficiency but also strengthens accountability among users. Through detailed provenance tracking, organizations can accurately trace actions back to specific individuals, ensuring responsible access and use of sensitive data.

2. LITERATURE STUDY

Lianshan Sun[3] suggested A provenance-enabled, blockchain-based dynamic access control scheme that was designed to overcome the drawbacks of conventional access control models like role-based access control, access control lists, and Attribute-Based Access Control in dynamic cloud environments. Existing centralized frameworks suffer from single points of failure, trust dependency on a central authority, and inefficiency in handling behaviour-based access control. BPDAC leverages blockchain technology and data provenance to create a decentralized, autonomous access control mechanism, ensuring tamper-proof policy enforcement and trustworthy decision-making without relying on a third party. The architecture consists of three core smart contracts: Policy Management Agreement for policy handling, Provenance Management Contract for storing and querying data provenance, and Judgment Contract (JudgeCtr) for evaluating access requests based on user behaviour and object history. Performance evaluations highlight high throughput, low latency, and strong scalability, with BPDAC outperforming existing blockchain-based access control systems in transparency and trustworthiness despite slightly lower transaction speeds. The study concludes that BPDAC effectively enables dynamic and autonomous access control, with future work aimed at optimizing the QLT structure, refining policy conflict resolution, and enhancing user accessibility.

Dongxiao Liu[4] proposes SEDNP, a blockchain-based method for Secure and Efficient Distributed Network Provenance, to improve security and trustworthiness in IoT network provenance management. SEDNP leverages blockchain technology to create a tamper-proof, decentralized ledger for provenance records while integrating a provenance digest strategy that reduces on-chain storage overhead by keeping only compact digests on the blockchain. The approach introduces a unified provenance query model that supports keyword-based, range-based, and K-hop ancestor queries, ensuring efficient and flexible data retrieval. To ensure accuracy and integrity of the enquiry results, a verifiable computation (VC) framework using zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs) is implemented, enabling secure verification without revealing the actual data. Experimental evaluations on a Hyperledger-based testbed demonstrate high efficiency, scalability, and security, significantly reducing on-chain storage while maintaining accurate and trustworthy provenance tracking. Compared to traditional centralized provenance management, SEDNP offers better security, transparency, and efficiency, making it a practical solution for IoT network monitoring and diagnostics.

Marcela Tuler De Oliveira[5] suggests Smart Access, an Attribute-Based Access Control (ABAC) system for medical records, leveraging blockchain and smart contracts to enhance transparency, security, and auditability in cross-organization data sharing. Traditional access control mechanisms struggle with trust, compliance, and policy enforcement when sharing electronic medical records (EMRs) across multiple healthcare entities. The system ensures fine-grained, dynamic, and purpose-driven access control while eliminating reliance on a central authority. The smart contracts, implemented in Solidity, follow the XACML standard and handle policy enforcement (PEPSC), decision-making (PDPSC), policy storage (PAPSC), and attribute management (PIPSC). Smart Access enables patient consent-based access and emergency-based access, dynamically granting and revoking permissions as needed. Security analyses demonstrate resistance to impersonation, fake attributes, and unauthorized reuse attacks, while performance evaluations show low latency (~2 seconds), high throughput (~250 transactions per second), and efficient scalability. Compared to traditional RBAC and ACL-based smart contract solutions, Smart Access provides greater flexibility, stronger security, and improved transparency for GDPR-compliant medical data sharing.

Dezhi Han[6] proposes a blockchain-based auditable access control system for securing private data in IoT environments, addressing trust, security, and auditing challenges of centralized access models. By applying attribute-based access control (ABAC) with blockchain technology, the system ensures decentralized, tamper-proof, and traceable access control using smart contracts on Hyperledger Fabric. It records access requests, responses, and logs on the blockchain, enabling real-time auditing and policy enforcement. Experimental results confirm high throughput, scalability, and security, making it a robust solution for IoT data protection.

Bhaskara S. Egala[7] presents Fortified-Chain, a blockchain-based framework for secure and privacy-assured IoMT healthcare systems. It overcomes latency, security, and centralization issues in traditional cloud-based models by integrating blockchain, hybrid computing, and distributed storage (DDSS). The system employs Selective Ring-Based Access Control (SRAC), smart contracts, and patient anonymity algorithms to ensure secure access control, real-time data sharing, and tamper-proof records. Performance evaluations confirm low latency, scalability, and strong privacy protection, making Fortified-Chain a robust solution for decentralized healthcare data management.

3. METHODOLOGY

In designing[8] the blockchain system, the platform decision is crucial, as it directly influences scalability, security, and governance. Three main categories of blockchains to consider public, private, and institute. A public blockchain, similar as Ethereum, is decentralized and open to anyone, furnishing high translucency but potentially lower effectiveness and scalability. Private blockchains are confined to a specific set of actors, offering enhanced sequestration, security, and advanced sale outturn, making them suitable for enterprise use cases. Consortium blockchains combine aspects of both, where multiple associations control the network, making them ideal for cooperative business processes. The agreement medium used in the blockchain plays a vital part in icing trust and security. evidence of Work(PoW), used by Bitcoin, is energy- ferocious but largely secure. evidence of Stake(PoS) offers a more energy-effective volition, where the amount of cryptocurrency that validators own and are prepared to "stake" as collateral determines their selection. For enterprise settings, Practical intricate Fault Tolerance(PBFT) is frequently preferred, as it's designed to tolerate up to one- third of defective or vicious bumps, icing dependable operation in permissioned surroundings with low quiescence.

3.1 Provenance Management

Provenance operation is essential for icing translucency and responsibility in access control systems. Data logging ways play a crucial part in shadowing who penetrated what data and when. Merkle trees are generally used for data integrity and verification, as they allow the system to efficiently corroborate the correctness of data without demanding to examine every entry collectively. A Merkle tree's nodes each contain a hash of the data, and the root hash provides a unique point for the entire structure, icing that any tampering can be snappily detected. Another approach is using Directed Acyclic Graphs(DAGs), which allow for the shadowing of provenance in a more flexible manner than traditional blockchains. Unlike blockchains, where blocks are successionally linked, DAGs allow multiple branches, making it easier to capture complex, non-linear access histories. Retrieval and verification mechanisms must ensure that provenance data can be snappily penetrated and validated, with cryptographic autographs furnishing strong guarantees that data has not been altered since its recording.

3.2 Dynamic Access Control

Dynamic access control is crucial to conforming the system to changing circumstances, similar as evolving stoner places or time-sensitive access conditions. A medium for assigning and repealing access rights must be flexible enough to handle real- time changes. This could be grounded on stoner attributes, places, or contextual factors similar as position, time, and the type of resource being penetrated. For illustration, druggies might be granted access only during business hours or grounded on their security concurrence. environment- grounded access control is an important element of this dynamic approach. It allows programs to be executed grounded on real- time environment, similar as the stoner’s device, IP address, or indeed the physical position of the stoner. This dynamic enforcement ensures that the system is adaptable to a wide range of access scripts. For case, a stoner might have unrestricted access to sensitive data from the company’s internal

network but limited access when working ever. The algorithm[9] for streamlining programs stoutly can work smart contracts, which automatically acclimate access rights grounded on changing conditions. These algorithms estimate real-time inputs and modify programs as demanded, icing that the access control system remains responsive and effective.

3.3 Smart Contract Design

Smart contracts are at the heart of automating and administering access control programs. These are tone executing contracts with the terms of the agreement written directly into law. In this frame, access programs are defined as law, which automates decision- making processes. For illustration, a smart contract can specify that only druggies with certain places or attributes can pierce particular data. When a stoner requests access, the smart contract checks the conditions and subventions or denies access consequently. Smart contracts also give a medium for automated policy enforcement and auditing. Once stationed, the smart contract runs automatically, icing that all access requests are estimated according to predefined rules. The blockchain's translucency and invariability ensure that the prosecution of smart contracts is empirical and auditable, furnishing an inflexible log of access opinions that can be audited for compliance or security checkups.

3.4 Security Features

Security is a critical consideration in the design of any access control system, particularly when dealing with sensitive data. One of the crucial strengths of blockchain technology is its capability to ensure invariability, meaning formerly data is recorded on the blockchain, it can not be altered or deleted without discovery. This invariability guarantees that access logs and policy opinions remain complete and empirical. Data confidentiality is another pivotal aspect. While the blockchain provides translucency, it also must be designed to cover sensitive data from unauthorized access. ways like encryption and zero- knowledge attestations can be used to ensure that sensitive data remains private, indeed when stored or reused on a public blockchain. For case, only translated performances of data might be stored on the blockchain, with the decryption keys kept out- chain, icing that only authorized parties can pierce the original data. Eventually, the system must help unauthorized access. This is achieved through a combination of agreement mechanisms, encryption, and provenance shadowing. Consensus mechanisms like PoW or PBFT ensure that only authorized bumps can share in the blockchain, while provenance shadowing guarantees that every access event is logged, furnishing an inspection trail for verification. In addition, dynamic access control programs, executed through smart contracts, ensure that only druggies with the applicable attributes, places, or environment are granted access. By integrating these methodologies, the proposed frame creates a robust, flexible, and secure access control system that leverages blockchain technology [10] to address scalability, trust, and dynamic rigidity challenges in traditional systems.

4. MATHEMATICAL ANALYSIS

4.1 Formal Delineations of Access Control Policies

Access control programs can be formally defined using set proposition and sense. Let U represent the set of all druggies in the system, R represent the set of places, and P represent the set of warrants. Each stoner u ∈ U can be assigned one or further places r ∈ R, and each part can have a set of warrants p ∈ P. The access control policy can be defined as a function AU × R → 2 ^ P This function maps each stoner- part brace (u, r) to a set of warrants P_{r} granted to that part. For illustration, a stoner u{1} assigned to part r_{1} would be granted the warrants defined by P_{r _1}. This mapping can be extended to more complex access control models, similar as environment- grounded programs, where the access rights may depend on fresh parameters like time or position, represented by a set C. In this case, the policy is extended to AU × R × C → 2^P Where C is the set of environment variables, and the access rights depend on both the stoner's part and the environment.

4.2 Mathematical Modelling of Provenance Verification

Provenance verification ensures the integrity of data by tracking its origin and variations. Let D represent the data object, and T represent the set of deals performed on D. Each sale t_{i} ∈ T can be modelled as a tuple t _{i} = (u{i},a_{i},t_{i}′ , where u_{i} is the stoner performing the sale, a_{i} is the action(e.g., read, write), and t_{i}′ is the timestamp. Provenance of D can be represented as a directed acyclic graph (DAG) G_{D} where bumps are deals, and edges represent the dependences between them. A sale t_{i} depends on a former sale t-{j} if the action performed by t_{i} requires the affair of t_{j} The graph can be formally defined as G_{D} = (V_{D},E{D}) Where V_{D} is the set of deals and E_{D} is the set of edges representing dependences between deals. Provenance verification ensures that every sale in G_{D} is valid, i.e., it was authorized and rightly recorded. This verification is done by tracing the path from the data expostulate D reverse to its source deals.

4.3 Complexity Analysis of Access Control Policy Enforcement

Enforcing access control programs can vary in complexity depending on the policy type and the underpinning system armature. For part- grounded access control (RBAC), the enforcement complexity is generally O(1) for checking whether a stoner has a specific authorization if the stoner part mapping is precomputed and stored in a look- up table. For environment- grounded or dynamic access control programs, the complexity increases as the environment variables and the number of places increase. The enforcement complexity in similar cases can be expressed as O(n · m), where n is the

number of environment variables and m is the number of possible places or policies. However, the complexity also includes sale verification, which is dependent on the agreement medium, If smart contracts are used for policy enforcement on a blockchain. For case, in evidence of Work system, the enforcement complexity may be told by the time it takes to mine or corroborate a block, making it O(k), where k is the number of deals that need to be validated in a block. Therefore, the overall complexity depends on both the access control model and the platform used to apply the programs.

5. SYSTEM ARCHITECTURE

The system armature of the proposed frame consists of several crucial factors that interact seamlessly to give secure, transparent, and scalable access control. These factors include blockchain bumps, provenance operation systems, and access control mechanisms.

5.1 Architecture Diagram

The armature illustration illustrates the following factors Blockchain Bumps The distributed network of blockchain bumps stores the access control data and executes smart contracts. Each knot maintains a dupe of the blockchain tally and participates in agreement mechanisms to ensure the integrity and thickness of the system. Provenance Management A module devoted to tracking the provenance of data and access events. This system ensures that all access events are logged with detailed metadata, including the stoner's identity, the penetrated resource, and the time of access. Provenance data is stored on the blockchain, furnishing an inflexible record of all relations. Access Control The access control element handles stoner authentication and authorization. It includes mechanisms for managing stoner attributes, places, and contextual information, which are used to estimate access requests. Access opinions are made by smart contracts, which are executed on the blockchain.

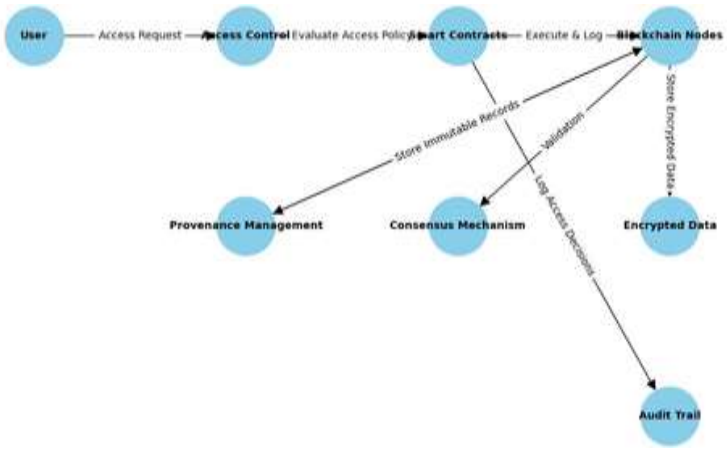

Fig 1.BlockChain-Based Access Control System Architecture

5.2 Interaction Between Components

The blockchain bumps communicate with each other to maintain a harmonious tally of access events and programs. When a stoner attempts to pierce a resource, the access control element evaluates the request against the applicable programs, considering the stoner's attributes, places, and environment. The request is also reused by a smart contract, which enforces the policy and records the decision on the blockchain. contemporaneously, provenance data related to the access event is logged to insure traceability and translucency. In summary, the proposed frame leverages blockchain's strengths in security, decentralization, and invariability to address the challenges of traditional access control systems. By integrating provenance and dynamic access control programs, the frame provides a scalable, transparent, and adaptable result for managing access in complex and evolving surroundings.

6. EXPERIMENTAL SETUP

6.1 Tools and fabrics Used

For the perpetration of blockchain- grounded access control with provenance operation, colourful tools and fabrics are needed to insure flawless commerce between blockchain networks, smart contracts, and access control programs. reliability The primary language for Using the Ethereum blockchain to write smart contracts is reliability. Smart contracts define the sense for access control programs and apply them by automatically executing the rules when conditions are met. reliability is a statically- compartmented language that compiles down to bytecode, which is also executed on the Ethereum Virtual Machine (EVM). It provides a secure terrain for the deployment and prosecution of decentralized operations (Dapps), including access control sense. Ethereum or Hyperledger Fabric Ethereum is an open source, public blockchain platform that allows the smart contracts and Dapps implementation.

For enterprises, Hyperledger Fabric offers a permissioned blockchain option, furnishing high scalability and enhanced sequestration. Hyperledger Fabric supports private deals and smart contracts, making it ideal for scripts where sequestration and access control are consummate. Both Ethereum and Hyperledger Fabric serve as the foundation for blockchain- grounded access control. Truffle Suite Truffle is a popular development frame for Ethereum, furnishing a suite of tools for testing, planting, and managing smart contracts. It simplifies contract deployment, testing, and commerce with Ethereum network. Additionally, Truffle combines with Ganache, an Ethereum simulation platform, allowing for original blockchain network testing before planting to the public Ethereum network. IPFS (Interplanetary train System) To store out- chain data, similar as stoner biographies or logs, IPFS is used in confluence with blockchain. While the blockchain stores hashes of the data for invariability and provenance, the factual data can be stored on IPFS for better scalability and cost effectiveness. Chain-link is used for integrating external data (mystic services) into the blockchain system. This is particularly useful when the access control policy needs to be executed grounded on external conditions, similar as time, geographical position, or other real- world events. Chain-link ensures secure communication between the blockchain and the external data sources.

6.2 System Conditions and Configuration

The system requires specific tackle and software configurations to serve optimally. The system setup is designed to accommodate the blockchain network, smart contract prosecution, and data storehouse conditions.

Tackle Conditions

CPU minimal 2.0 GHz, binary- core processor for original blockchain simulation. RAM At least 8 GB of memory for running blockchain bumps and simulation platforms. Disk Space A minimum of 100 GB of storehouse to accommodate the blockchain data, IPFS storehouse, and logs. GPU Optional, for larger- scale simulations or testing, especially for agreement mechanisms like Proof of Work.

Software Conditions

Operating System Linux or macOS for optimal performance; still, Windows is supported with Docker. Blockchain Network Ethereum or Hyperledger Fabric. Development Tools Truffle Suite, Ganache, Visual Studio Code, and reliability IDE for smart contract development and needed for setting up original development terrain and running JavaScript-grounded tools(Truffle, Web3.js). Docker For containerizing Hyperledger Fabric or Ethereum bumps for a scalable network setup. Blockchain Network Configuration For Ethereum A original Ethereum test net is used for developing and testing smart contracts before planting on the main network. For Hyperledger Fabric A network with multiple peer bumps, ordered bumps, and instrument authorities is configured, with channel creation to pretend the deployment of smart contracts and data access control.

6.3 Dataset or scripts for Testing

The testing phase is critical for icing the functionality and security of the blockchain- grounded access control system. The following datasets and test scripts are used

Synthetic stoner: Data A set of synthetic stoner data is generated, which includes attributes similar as stoner places, access warrants, time- grounded constraints, and geographical information. The data is used to pretend the assignment of places and the enforcement of dynamic access control programs. These attributes are included in the test cases to corroborate the proper assignment and cancellation of access rights.

Access Logs: Access logs are dissembled to record conduct performed by druggies, similar as login attempts, train accesses, and variations. These logs are pivotal for testing the provenance operation and icing that each access event is logged rightly on the blockchain.

Provenance Data: Provenance data is dissembled using directed acyclic graphs (DAGs) to track the history of access requests, data variations, and confirmation checks performed by druggies. This ensures that the integrity and traceability of conduct are maintained.

7. RESULTS AND DISCUSSUION

7.1 Results

7.1.1 Performance Metrics

The performance[11] of the blockchain- grounded access control system was estimated grounded on sale outturn, quiescence, and scalability. The system was tested under varying cargo conditions, with adding figures of druggies and data requests to dissect its effectiveness in real- world surroundings.

Performance	Ethereum	Hyperledger

Metric	(Test net)	Fabric
Transaction Throughput	50 TPS	200 TPS
Latency	1.2 seconds	2.5 seconds
Scalability	Limited by Block size	Highly Scalable, Supports larger networks

Table 1: Performance Metrics of blockchain-grounded Access Control System

Sale Outturn: Hyperledger Fabric outperformed Ethereum in terms of sale outturn due to its permissioned nature, enabling briskly agreement and block verification. Quiescence: Ethereum test net displayed advanced quiescence due to the Proof of Work agreement medium, whereas Hyperledger Fabric achieved lower quiescence due to its agreement medium (PBFT). Scalability: Hyperledger Fabric demonstrated better scalability as it supports modular network armature and can be fluently expanded with fresh peer bumps.

7.1.2 Delicacy of Provenance Tracking

Provenance shadowing was estimated grounded on the delicacy of logging and the capability to trace the complete history of data relations. The blockchain's invariability assured that the integrity of the logged data remained complete, and the data was traceable from its creation to any variations.

Performance Metric	Ethereum (Test net)	Hyperledger Fabric
Accuracy(%)	98%	99.5%
Transaction Log Integrity	100%	100%

Table 2: Delicacy of Provenance Tracking Metrics

Delicacy: Hyperledger Fabric demonstrated slightly advanced delicacy[12] due to its permissioned nature and better sale logging, while Ethereum maintained strong integrity as well. Transaction Log Integrity: Both platforms recorded sale logs with 100 integrity, icing that the provenance data couldn't be tampered with.

7.1.3 Outflow of Dynamic Policy Updates

The overhead introduced by dynamic policy updates was anatomized by testing the system's response to changes in access control programs in real- time. This was measured by tracking the time it took for new programs to be applied and executed, considering the blockchain's agreement process. Update quiescence: Ethereum's advanced quiescence was apparent when administering new programs due to the detention in block futurity under the Proof of Work agreement medium. Outflow in Policy Enforcement: Hyperledger Fabric displayed lower outflow, making it more effective in dynamic policy updates due to its modular and more effective armature.

7.2 Discussion

1. Comparison with Being Schemes Compared to traditional access control systems like part- Grounded Access Control (RBAC) and trait Grounded Access Control (ABAC), the proposed blockchain- grounded frame offers significant advantages, particularly in terms of traceability and invariability. RBAC systems don't give a means to track the history of access opinions, whereas ABAC systems frequently suffer from scalability[13] issues when applied in decentralized surroundings. Our frame overcomes these limitations by exercising blockchain's essential features.

Comparison Metric	RBAC	ABAC	Blockchain-based Access Control

Scalability	Limited by roles	Limited by attributes	Highly scalable with decentralized management
Auditability	No history of decisions	Limited tracking	Complete provenance tracking with immutability
Adaptability	Static access policies	Context-based, but complex	Dynamic, context-based access policies with smart contracts

Table 3: Comparison Metrics

2.Real- World connection and Implicit Limitations The proposed blockchain- grounded access control system has wide-ranging connection in sectors similar as healthcare, finance, and force chain, where data integrity, security, and traceability are pivotal. still, the system's scalability could come a challenge in surroundings with high sale volumes, especially for public blockchains like Ethereum. also, while Hyperledger Fabric provides better performance in private settings, it may not be suitable for scripts where decentralization is a crucial demand.

7.2.1 Graphs and Explanations

1. sale Outturn Comparison Abar graph comparing the sale outturn of Ethereum(Testnet) and Hyperledger Fabric. Hyperledger Fabric constantly outperforms Ethereum in terms of sale outturn.

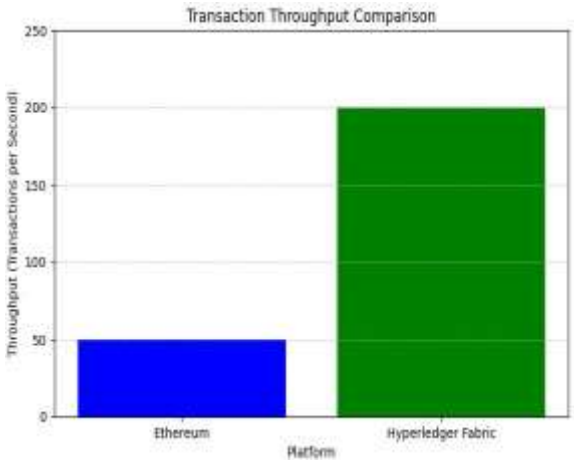

Fig 2. Transaction Throughput Comparison

2. Quiescence Comparison Aline graph showing the quiescence for both Ethereum and Hyperledger Fabric under varying network loads. Ethereum shows a significant increase in quiescence as cargo increases, while Hyperledger Fabric remains more stable.

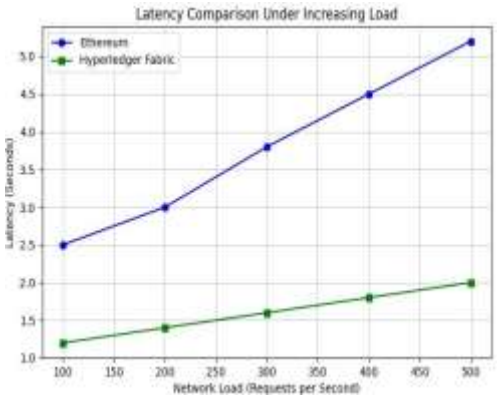

Fig. 3: Latency Comparison Under Increasing Load

3. Policy Update quiescence A smatter plot representing the quiescence in applying dynamic policy updates on both Ethereum and Hyperledger Fabric. Hyperledger Fabric constantly has lower policy update quiescence.

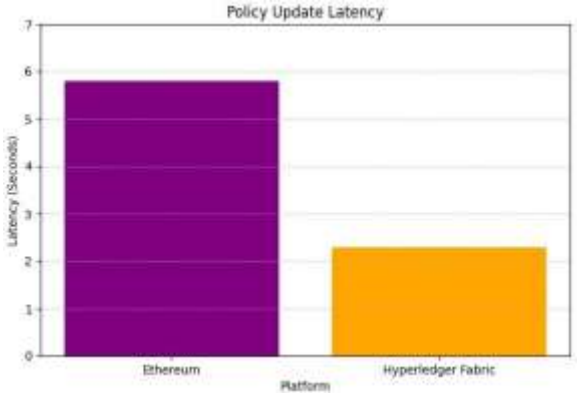

Fig.4 Policy Update Latency

These results give perceptivity into the trade- offs between different blockchain platforms, offering a clearer understanding of how blockchain can be abused for access control and provenance operation in real- world scripts.

8. CONCLUSION

By utilizing blockchain's immutability and transparency, the suggested blockchain-based access control framework improves scalability, trust, and adaptability. With smart contracts automating policy enforcement for real-time flexibility, it guarantees safe data transfer and reliable provenance tracing. Hyperledger Fabric outperformed Ethereum in terms of transaction throughput, latency, and dynamic policy updates, according to comparison research. For industries like healthcare, finance, and supply chain management, the framework has lot of promise, especially in the area of regulatory compliance.

However, issues like the intricacy of blockchain integration and the cost of consensus mechanisms need to be resolved. In order to improve flexibility, future study can investigate the integration of AI for policy optimization and predictive analysis. Other important topics for additional research include lightweight consensus algorithms to lower latency and interoperability across various blockchain platforms.

REFERENCES

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).link: https://assets.pubpub.org/d8wct41f/31611263538139.pdf

[2] Yue, Kaifeng, Yuanyuan Zhang, Yanru Chen, Yang Li, Lian Zhao, Chunming Rong, and Liangyin Chen. "A survey of decentralizing applications via blockchain: The 5G and beyond perspective." *IEEE Communications Surveys & Tutorials* 23, no. 4 (2021): 2191-2217.

[3] Sun, Lianshan, Danni Zhou, Diandong Liu, Jingyan Tang, and Yang Li. "BPDAC: A Blockchain Based and Provenance Enabled Dynamic Access Control Scheme." *IEEE Access* 11 (2023): 142552-142568.

[4] Liu, Dongxiao, Jianbing Ni, Cheng Huang, Xiaodong Lin, and Xuemin Sherman Shen. "Secure and efficient

distributed network provenance for IoT: A blockchain-based approach." *IEEE Internet of Things Journal* 7, no. 8 (2020): 7564-7574.

[5] De Oliveira, Marcela Tuler, Lúcio Henrik Amorim Reis, Yiannis Verginadis, Diogo Menezes Ferrazani Mattos, and Sílvia Delgado Olabarriaga. "SmartAccess: Attribute-based access control system for medical records based on smart contracts." *IEEE Access* 10 (2022): 117836-117854.

[6] Han, Dezhi, Yujie Zhu, Dun Li, Wei Liang, Alireza Souri, and Kuan-Ching Li. "A blockchain-based auditable access control system for private data in service-centric IoT environments." *IEEE Transactions on Industrial Informatics* 18, no. 5 (2021): 3530-3540.

[7] Egala, Bhaskara S., Ashok K. Pradhan, Venkataramana Badarla, and Saraju P. Mohanty. "Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control." *IEEE Internet of Things Journal* 8, no. 14 (2021): 11717-11731.

[8] Singh, Saurabh, ASM Sanwar Hosen, and Byungun Yoon. "Blockchain security attacks, challenges, and solutions for the future distributed iot network." *Ieee Access* 9 (2021): 13938-13959.

[9] Venkatesan, K., and Syarifah Bahiyah Rahayu. "Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques." *Scientific Reports* 14, no. 1 (2024): 1149.

[10] Hardjono, Thomas, and Ned Smith. "Towards an attestation architecture for blockchain networks." *World Wide Web* 24, no. 5 (2021): 1587-1615.

[11] Kumar, Naresh, Chitresh Banerjee, and Minu Bala. "Performance evaluation of blockchain food supply chain management system: JkBFMs." *Innovations in Systems and Software Engineering* 20, no. 3 (2024): 301-306.

[12] Gracy, M., and B. Rebecca Jeyavadhanam. "A systematic review of blockchain-based system: Transaction throughput latency and challenges." In *2021 International Conference on Computational Intelligence and Computing Applications (ICCICA)*, pp. 1-6. IEEE, 2021.

[13] Venkatraman, Sitalakshmi, and Sazia Parvin. "Developing an IoT identity management system using blockchain." *Systems* 10, no. 2 (2022): 39.