Journals Pub

International Journal of
Distributed Computing and Technology

ISSN: 2455-7307
Volume 12, Issue 1, 2026
January–June
DOI (Journal): 10.37628/IJDCT

https://journalspub.com/journal/ijdct/

Review IJDCT

A Study on Securing the Local Area Network with the Immutable Trust of Blockchain

Vaishnavi Gopal Shirsikar[1,*], Aditi Dinanath Shahane[1], Kazi Kutubuddin Sayyad Liyakat[2]

Abstract

The contemporary Local Area Network (LAN) is the digital circulatory system of the modern enterprise, a vital yet perilously vulnerable ecosystem. Traditional security paradigms, built upon centralized authority models – firewalls, intrusion detection systems, and privileged administrators – increasingly resemble medieval castles in an age of artillery. They present a brittle single point of failure: compromise the center, and the entire kingdom falls. This paper proposes a radical architectural shift, envisioning the LAN not as a fortress to be defended, but as a consensus-driven organism to be verified. We introduce a novel framework for LAN security leveraging the foundational principles of blockchain technology: decentralization, immutability, and cryptographic auditability. Our methodology involves the implementation of a private, permissioned blockchain overlay atop the existing physical network infrastructure. In this model, every network device – from endpoints and servers to switches and routers – acts as a node participating in a continuous, low-latency consensus mechanism. Core network functions – device authentication, address allocation via DHCP – and access control policy enforcement – are transformed into smart contracts. These self-executing contracts autonomously validate requests against a distributed ledger, ensuring that only authorized, cryptographically-verified entities can join or interact within the network. This eradicates the threat of spoofing, rogue device infiltration, and malicious lateral movement by making every action transparent, contestable, and irrevocably logged. By dismantling the centralized chokepoints of conventional security, we architect a LAN that is not merely protected, but inherently trustworthy by design.

Keywords: Blockchain, decentralized identity and access control (DIAC), distributed ledger technology (DLT), local area network, security

INTRODUCTION

The total security infrastructure of the modern Local Area Network (LAN) is wrestling with an existential crisis. Born in the age of monolithic servers and corporate perimeters, traditional access control and logging systems are buckling under the weight of Internet of Things (IoT), aggressive BYOD policies, and the pervasive shift toward Zero Trust architectures [1].

The core vulnerability remains centralization. When your identity management, security logs, and access policies reside on a single server – the Active Directory, the central SIEM, or the master firewall – you create a single, high-value target for attackers.

A decentralized architecture is needed to secure an inherently decentralized environment. The solution lies in a technology engineered specifically

***Author for Correspondence**
Vaishnavi Gopal Shirsikar
E-mail: rajasaheb.3617@gmail.com

[1]Assistant Professor, Department of Electronics and Telecommunication, Brahmdevdada Mane Institute of Technology, Solapur, Maharashtra, India
[2]Professor and Head, Department of Electronics and Telecommunication, Brahmdevdada Mane Institute of Technology, Solapur, Maharashtra, India

Received Date: November 14, 2025
Accepted Date: November 19, 2025
Published Date: February 02, 2026

Citation: Vaishnavi Gopal Shirsikar, Aditi Dinanath Shahane, Kazi Kutubuddin Sayyad Liyakat. A Study on Securing the Local Area Network with the Immutable Trust of Blockchain. International Journal of Distributed Computing and Technology. 2026; 12(1): 24–35p.

for distributed trust: the blockchain. For decades, LAN protection relied on the "M&M" security model: Hard on the outside (firewalls and VPNs), soft on the inside (easy lateral movement once an attacker is authenticated) [2].

THE BOTTLENECK OF IDENTITY MANAGEMENT

Traditional Identity and Access Management (IAM) systems must constantly query a single central authority. If that central server is compromised, denied, or simply overwhelmed, the entire system of trust collapses. Furthermore, every single device added to the network (be it a smart thermostat or a new laptop) requires manual registration and management, leading to sprawl and human error.

The Fragility of Audit Trails

Security audits and detailed forensic investigations rely entirely on the integrity of log files. A sophisticated attacker, once achieving root access, can alter or delete key event logs to cover their tracks. Without verifiable, immutable logging, the backbone of forensic security is inherently flawed.

Lateral Movement Risk

Once inside the network perimeter, an authenticated user or compromised device can often move freely (laterally) toward high-value assets. Legacy segmentation tools struggle to keep pace with the hyper-dynamic nature of modern traffic flow.

Blockchain technology, in the context of a LAN, is not about cryptocurrency. It is a distributed ledger, verified by consensus, that replaces the central security registrar. By implementing a private, permissioned blockchain (such as Hyperledger Fabric or a specialized enterprise ledger) within the network, security functions are distributed to every point of presence, making the system resilient and immutable [3–5].

Here are the three primary applications transforming lan security:

1. Decentralized Identity and Access Control (DIAC)

In a modern blockchain-managed LAN, identity is no longer granted by a single Active Directory server; it is verified by the entire network.

- *How It Works:* Every user and device wishing to access the network is assigned a unique, cryptographic identity (a wallet address or DID – Decentralized Identifier). When a user attempts to connect, the request is broadcast to nearby nodes (switches, routers). These nodes consult the distributed ledger to verify the digital certificate and the current access policy associated with that DID.
- *The Power of Immediate Consensus:* If a device is detected performing malicious activity, the security policy regarding its DID can be instantly updated on the blockchain. Because the ledger is distributed, every network device immediately recognizes that identity as compromised and denies access, eliminating latency and preventing the attacker from simply plugging into a different switch.

2. Immutable Log and Audit Trails (The Forensic Goldmine)

By writing security events to blockchain, organizations solve the log integrity paradox.

- *Forensic Assurance*: Every event – a login attempt, a policy change, a failed connection – is written as a block and cryptographically chained to the previous one. This creates a time-stamped, tamper-proof record. If an attacker gains root access and tries to delete their activities, the cryptographic hash of the chain would instantly break, alerting monitoring systems to the attempted manipulation.
- *Regulatory Compliance:* For industries with stringent compliance requirements (like finance or healthcare), blockchain provides an unassailable audit platform, proving that logs have not been altered after the fact.

3. Automated IoT and Micro-Segmentation

The massive proliferation of IoT devices (often deployed with poor security standards) presents the greatest threat to LAN stability. Blockchain provides a robust framework for managing trustless devices.

- *Automated Provisioning:* When a new IoT device is plugged in, it's not manually registered. It automatically broadcasts its identity request. The network's consensus mechanism verifies its credentials and instantly assigns it to an isolated micro-segment on the network, enforced by smart contracts [5–7].
- *Smart Contract Policy:* Access rules – defining what resources the device can communicate with, and for how long – are codified into a smart contract written on the ledger. If the device deviates from its predefined behavior (e.g., a printer starts trying to access the HR database), the smart contract automatically revokes its access and quarantines the device.

While the potential is indeed quite enormous, implementing a blockchain-based LAN involves significant practical challenges as shown in Table 1 that must be addressed:

Table 1. Practical challenges.

Challenge	Mitigation strategy
Latency and Throughput	Public blockchains are too slow. A LAN requires *sub-millisecond* verification. Solutions must use highly optimized, private, permissioned ledgers designed for high transaction speed and low consensus overhead.
Cost and Complexity	Integrating blockchain into existing network hardware (switches, routers) requires significant investment and the development of specialized middleware or custom firmware.
Scalability (Storage)	If every packet header or event log is written to the blockchain, the ledger will grow exponentially, quickly consuming storage. Solutions must focus on writing *only* security-critical metadata and policy changes, not raw traffic data.
Legacy Integration	Most organizations cannot rip out their entire infrastructure. Blockchain must be implemented incrementally, perhaps initially managing only IoT devices or specific high-security zones, while integrating with existing RADIUS/AAA servers.

Blockchain is not a replacement for traditional security tools like firewalls, VPNs, or antivirus software. It is a foundational trust layer – a crucial shift from perimeter-centric defense to identity-centric verification.

By decentralizing the source of truth, organizations gain a network that is inherently more resilient, forensically verifiable, and adaptive to modern threats. The eventual goal is a security system so distributed and automated that human intervention focuses only on policy creation, while the network itself – verified by the immutable ledger – becomes its own impenetrable guard. The firewall is dead; long live the distributed ledger [8, 9].

A BLOCKCHAIN FRAMEWORK FOR LAN SECURITY

The Local Area Network (LAN) is the absolute heart of many organizations, a vital artery pumping data and enabling collaboration. Yet, its relative proximity often makes it a tempting target for internal threats, compromised credentials, and sophisticated malware that bypasses perimeter defenses. Traditional LAN security, relying on firewalls, intrusion detection systems, and access control lists, is a crucial bulwark, but it can be fragmented, prone to human error, and struggles with transparent, immutable record-keeping.

Imagine a LAN where every connection, every data transfer, every device interaction is logged, verified, and tamper-proof. This is the promise of a Blockchain Framework for LAN Security. By decentralizing trust and creating an immutable ledger of network activity, we can build a more resilient, transparent, and auditable LAN environment [10, 11].

Here's a conceptual framework, outlining the key components and potential benefits:

- *Primary Permissioned Blockchain Network:* Unlike public blockchains, a permissioned blockchain is ideal for a LAN. Only authorized devices and administrators can join the network, ensuring control and privacy. This could involve a private enterprise blockchain solution or a consortium blockchain if multiple organizations share a network.

- *Smart Contracts as Security Agents:* These self-executing contracts, deployed on the blockchain, automate, and enforce security policies. They act as intelligent agents, continuously monitoring and responding to predefined conditions (Figure 1).
- *Distributed Ledger Technology (DLT):* Every validated transaction (e.g., device connection, file access, policy change) is recorded across multiple nodes (devices or dedicated servers) in the LAN, eliminating single points of failure and making it incredibly difficult to alter or delete records [12].

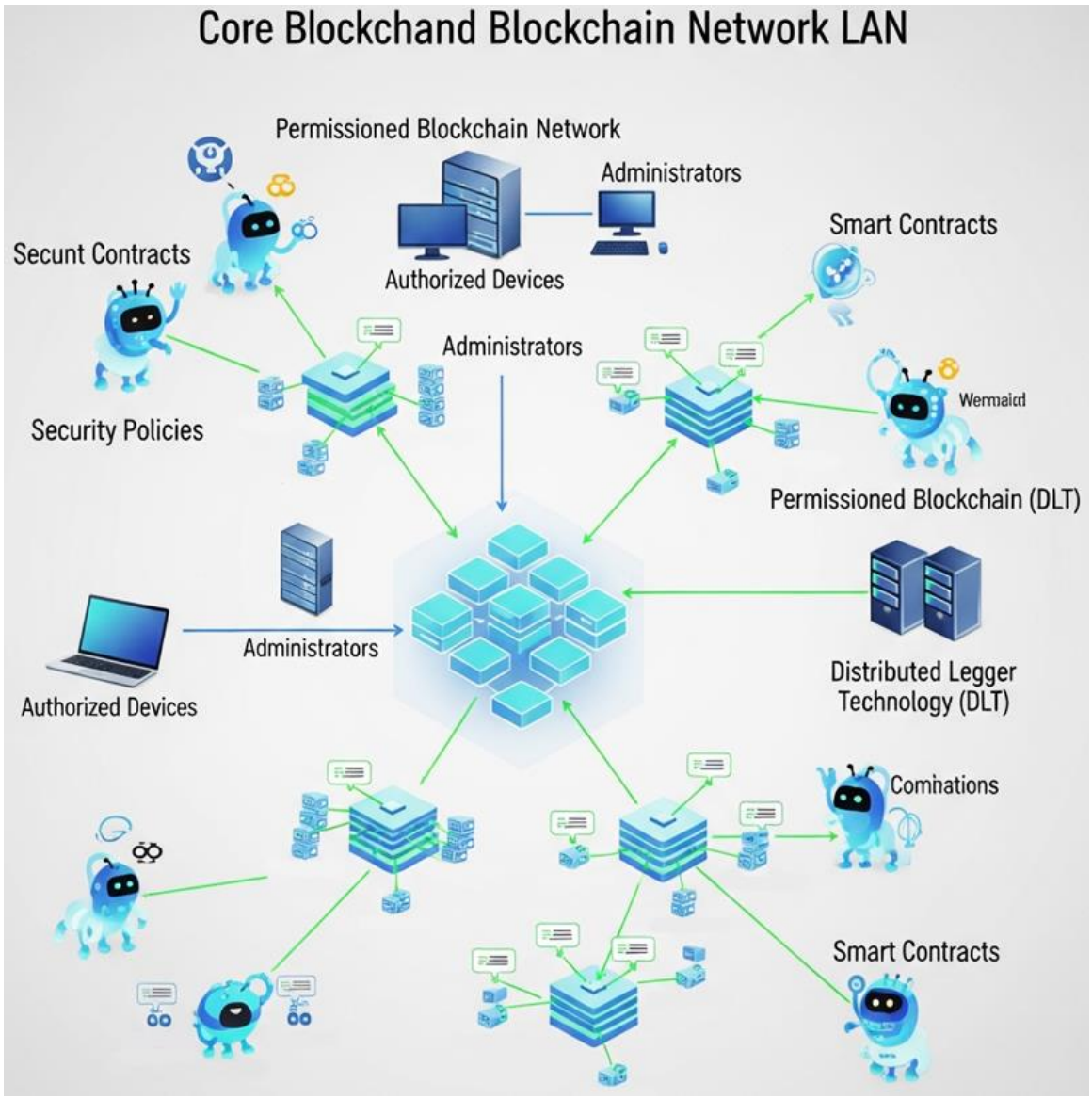

Figure 1. Blockchain enabled LAN.

Decentralized Identity and Access Management (DIAM)

- *Concept:* Instead of a centralized directory service (like Active Directory), each user and device are assigned a unique, verifiable digital identity on the blockchain.

Blockchain Integration

- *Identity Creation/Revocation:* New user/device identities are registered as transactions on the blockchain. Revocation is also a recorded transaction, making it immediately visible and auditable.
- *Access Control Policies:* Permissions are defined as smart contracts. When a user attempts to access a resource, the smart contract queries the blockchain for their verified identity and associated permissions.

- *Multi-Factor Authentication (MFA) Anchoring:* MFA challenges and successful authentications can be cryptographically signed and recorded on the blockchain, providing an immutable audit trail of access attempts (Figure 2).

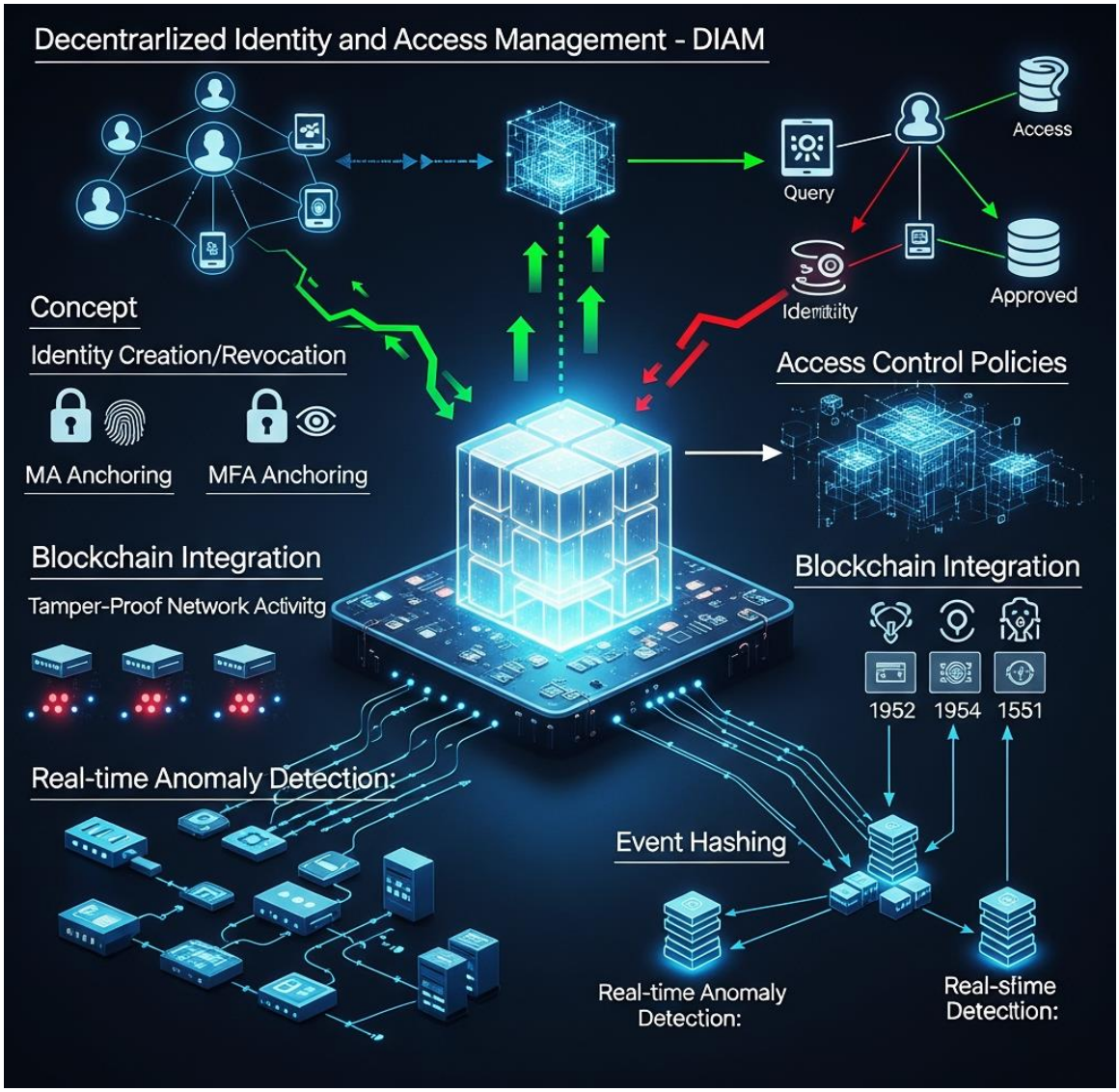

Figure 2. Component and integration of blockchain.

Tamper-Proof Network Activity Logging

- *Concept:* All significant network events – connection attempts, data transfers, protocol usage, configuration changes – are logged and hashed onto the blockchain.

Blockchain Integration

- *Event Hashing:* Instead of storing entire logs on-chain (which would be inefficient), critical events are hashed, and these hashes are periodically batched and recorded as transactions. This ensures the integrity of the full logs stored off-chain.
- *Real-time Anomaly Detection:* Smart contracts can monitor incoming event hashes. If a deviation from expected patterns is detected, it can trigger alerts or automated responses.
- *Forensic Analysis:* In case of a security incident, investigators can use the blockchain ledger to reconstruct events with absolute certainty, verifying the integrity of the data and identifying the sequence of actions.

Secure Configuration and Policy Management

- *Concept:* Network device configurations and security policies are managed and updated through a blockchain-based process.

Blockchain Integration

- *Version Control:* Every approved configuration or policy change is recorded as a transaction, creating an immutable version history.
- *Smart Contract Enforcement:* Smart contracts can verify that devices are running approved configurations and adhere to defined policies. Any deviation triggers an alert or remediation.
- *Decentralized Policy Updates:* Administrators can propose policy updates, which are then voted on by a designated group of authorized nodes. Once approved, the update is recorded on the blockchain and pushed to devices.

Device Health and Integrity Monitoring

- *Concept:* Devices within the LAN periodically report their health status and integrity checks (e.g., for malware, unauthorized software installations) which are anchored to the blockchain.

Blockchain Integration

- *Health Report Anchoring:* Device health reports are signed and hashed, with the hashes recorded on the blockchain.
- *Trust Scoring:* A decentralized trust score can be assigned to each device based on its history of verified health reports. Devices with low trust scores can be automatically quarantined or restricted.
- *Proactive Threat Mitigation:* If a device's health report is inconsistent with its historical data or deviates significantly, smart contracts can automatically initiate containment procedures.

Benefits of a Blockchain-Powered LAN Security Framework (Figure 3)

- *Enhanced Transparency and Auditability:* Immutable records provide absolute clarity on network activities, simplifying compliance and incident response.
- *Improved Data Integrity:* Hashing and distributed consensus prevent unauthorized modification of security logs and policies.
- *Reduced Risk of Single Point of Failure:* Decentralized architecture eliminates reliance on a single server for critical security functions. Automated Policy Enforcement: Smart contracts enable proactive and continuous enforcement of security rules.
- *Decentralized Trust:* Trust is not vested in a single administrator or system but distributed across the network through consensus mechanisms.
- *Greater Resilience Against Insider Threats:* Malicious insiders would find it significantly harder to tamper with logs or manipulate access controls without detection.

Challenges and Considerations

- *Scalability:* For very large LANs, efficiently processing and storing blockchain transactions will be critical. Layer 2 solutions and optimized consensus mechanisms will be necessary.
- *Complexity:* Implementing and managing a blockchain-based security framework requires specialized expertise.
- *Integration with Existing Infrastructure:* Seamless integration with legacy systems will be a significant undertaking.
- *Energy Consumption:* While permissioned blockchains are generally more energy-efficient than public ones, careful consideration of the consensus algorithm is still important.
- *Standardization:* A lack of universal standards for blockchain in network security could pose interoperability challenges.

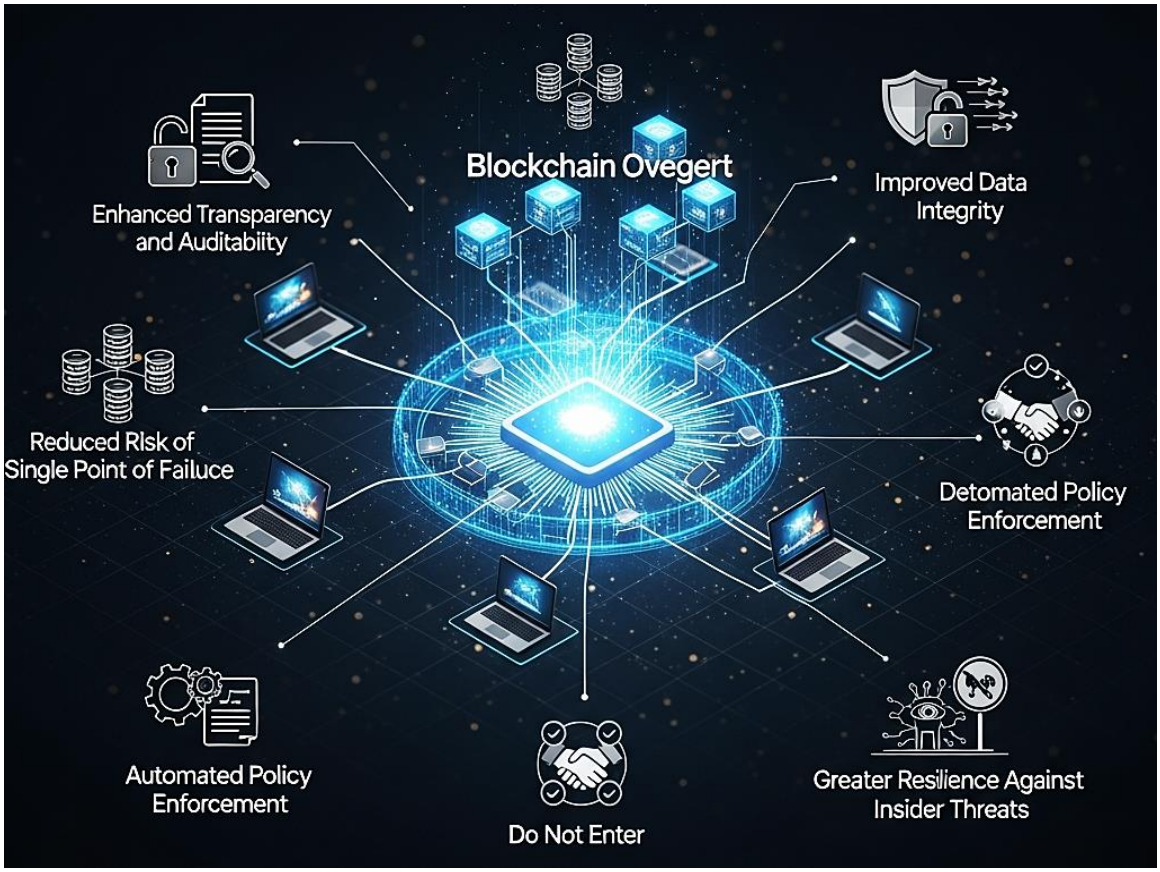

Figure 3. Benefits.

A blockchain framework for LAN security is not a silver bullet, but it offers a significant paradigm shift. By leveraging the inherent properties of decentralization, immutability, and transparency, organizations can build a LAN that is not only more secure but also more trustworthy and auditable. As the technology matures and adoption grows, we can anticipate a future where the local network perimeter is fortified with an unbreachable, intelligent, and continuously verified digital fortress. The age of the transparently secured LAN has begun.

BLOCKCHAIN IS DECENTRALIZING AND SECURING THE LAN

The traditional Local Area Network (LAN) has very long been protected by a "walled garden" approach: strong firewalls encircling a single, centralized authority – the authentication server. But in the age of global threats, remote work, and proliferating IoT devices, this centralized model is failing. A single point of failure (SPOF) is a catastrophic risk, making the network vulnerable to both external attacks and insider threats.

Enter the blockchain. Historically tethered to cryptocurrency, this distributed ledger technology (DLT) is rapidly emerging as the revolutionary architecture needed to build the next generation of resilient, trustless LAN security. By shifting the security paradigm from centralized control to decentralized consensus, we can finally build a digital fortress impervious to the compromise of any single component.

In legacy LAN environments, security, and access management rely on a central broker, typically a RADIUS server or Active Directory. This centralized structure faces three major vulnerabilities:

- *Single Point of Failure (SPOF):* If the authentication server is breached (e.g., via a successful phishing attack or Zero-Day exploit), the attacker gains the keys to the entire kingdom – all network access, logs, and policy controls are compromised simultaneously.

- *Log Tampering:* Security logs are stored locally or on a single logging server. A sophisticated attacker can delete or modify these logs to cover their tracks, hindering incident response and forensic analysis.
- *Inefficient IoT Onboarding:* Every new device, from smart HVAC systems to employee laptops, must be manually authenticated by the central authority. This process is time-consuming and introduces significant human error, leading to weak default configurations.

Blockchain's inherent properties of decentralization, immutability, and transparency provide a direct countermeasure to the weaknesses of centralized security. When applied to a LAN, the blockchain transforms from a financial register into a distributed, tamper-proof security ledger.

Here is how DLT fundamentally changes LAN security (Figure 4).

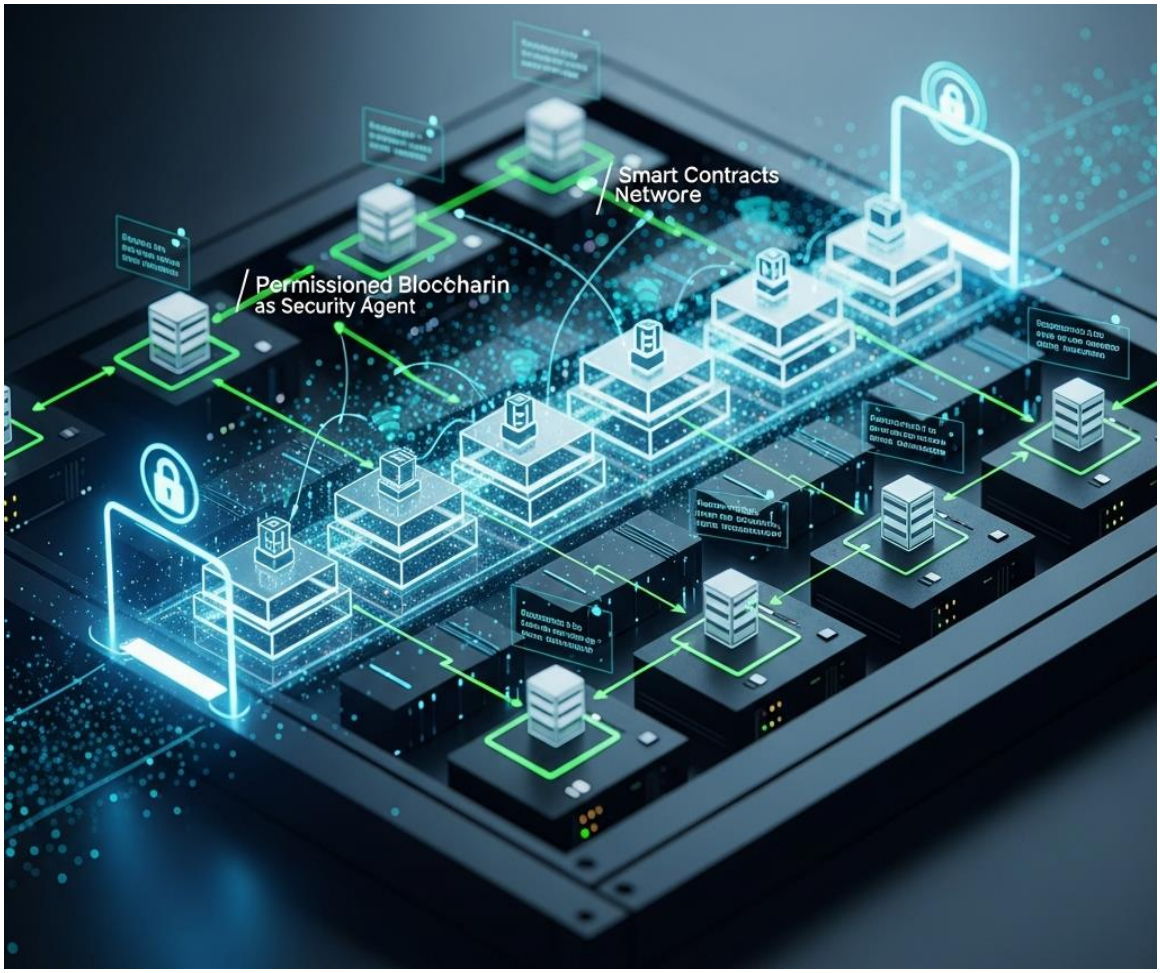

Figure 4. DLT in LAN security.

Decentralized Identity and Access Management (DIAM)

Instead of simply relying on a central server to verify a user's identity, the blockchain distributes this verification process across every node in the network.

- *Digital Signatures and Consensus:* Every device or user is assigned a cryptographic identity (often called a Decentralized Identifier or DID). When a user requests access, their key is published to the network. The distributed ledger validates the proof of identity based on the immutable record, confirming the user's rights without a central server needing to store the master password list.
- *Trustless Handshake:* This "trustless handshake" means that even if one node is compromised, the attacker cannot impersonate a user because the consensus mechanism of the remaining nodes will reject the fraudulent credential.

Immutable Policy Enforcement via Smart Contracts

In a traditional LAN, security policies (specifically who can access what) are housed in policy servers and firewalls, which can be manually overridden. Blockchain introduces the concept of Smart Contracts to automate and enforce these rules immutably.

A Smart Contract deployed on the LAN blockchain dictates specific access rules (e.g., "Device X can only communicate with Server Y during business hours"). Once these policies are codified and approved by consensus, they cannot be changed unless the network agrees to execute a specified governance mechanism. This eliminates the risk of an administrator secretly widening a security loophole for malicious purposes.

Transparent and Tamper-Proof Audit Trails

The most powerful and immediate application of blockchain in LAN security is its ability to secure audit logs. Every access attempt, every policy change, and every detected threat is recorded as a new block in the network chain.

Because the ledger is distributed and immutable, it is impossible for an attacker (or a disgruntled insider) to retroactively delete or alter logs. Any attempt to modify a block would immediately invalidate the entire chain of blocks held by the vast majority of nodes.

This provides a robust, verifiable chain of custody essential for stringent regulatory compliance (HIPAA, GDPR) and significantly streamlines forensic analysis following a breach.

The convergence of blockchain and LAN security is particularly transformative in two modern network scenarios:

Case 1: Securing the IoT Sprawl

The billions of IoT devices connecting to corporate networks often lack robust security features and are difficult to manage centrally.

- *Decentralized Onboarding:* New IoT devices can be onboarded directly to the blockchain. The network verifies the device's unique identifier (MAC address or UUID) and assigns it a limited-scope policy via a smart contract.
- *Micro-Segmentation:* The blockchain creates automatic, immutable micro-segments. For instance, a smart thermostat is only granted access to the HVAC server's API and is forbidden from communicating with the financial server – a policy enforced cryptographically by the DLT, not by a single firewall rule that could be misconfigured.

Case 2: True Zero Trust Architecture

Zero Trust operates on the principle of "never trust, always verify." Blockchain is the ideal foundational technology for achieving this mandate because it naturally facilitates constant, trustless verification.

- *Continuous Authentication:* Smart contracts can enforce conditional access, requiring re-authentication or re-verification upon changes in context (e.g., a user's device suddenly moves to a different geographical location).
- *Resilience:* If one segment of the Zero Trust network falls under attack, the blockchain ensures that the security policies for all other segments remain inviolable and operational, preventing lateral movement of the threat.

While the integration of DLT promises unmatched resilience, it is not without challenges. Implementing enterprise-grade blockchain solutions requires careful consideration of:

- *Scalability:* Processing millions of transactions (log events, access requests) per second require high-performance blockchain architectures, often utilizing private or consortium chains optimized for speed.
- *Computational Overhead:* Cryptographic verification is computationally intensive. The network must be designed to minimize latency while maintaining security.

Despite these hurdles, the inevitable trajectory of network security points toward decentralization. Blockchain offers a paradigm shift: moving security from a fragile core defended by firewalls to a resilient, distributed web of trust. By leveraging the power of the immutable ledger, organizations can stop chasing perimeter defense and start securing the individual identities and transactions that truly define the modern LAN.

Let's conceptualize the "program code" not as literal lines in Solidity or Go, but as the fundamental logic and smart contract structures that would underpin such a system. This is perhaps the most immediate and impactful application. Instead of a central RADIUS or Active Directory server, access policies are encoded directly into smart contracts.

Conceptual Code Snippet (Solidity-like):

```
// Smart Contract: AccessControlManager
contract AccessControlManager {
struct Device {
bytes32 deviceIDHash;
address ownerAddress;
string deviceType; // e.g., "Laptop", "IoT_Sensor", "Server"
string securityZone; // e.g., "DMZ", "Internal", "Guest"
bool approved;
}
struct User {
bytes32 userIDHash;
address userAddress;
string role; // e.g., "Admin", "Developer", "Guest"
uint lastLogin;
bool active;
}
mapping(bytes32 => Device) public registeredDevices;
mapping(bytes32 => User) public registeredUsers;
mapping(bytes32 => bytes32[]) public authorizedAccesses; // deviceIDHash => userIDHash[]
event DeviceRegistered(bytes32 indexed deviceIDHash, string deviceType);
event UserLoggedIn(bytes32 indexed userIDHash, bytes32 indexed deviceIDHash);
event AccessGranted(bytes32 indexed deviceIDHash, bytes32 indexed userIDHash, string resource);
event AccessDenied(bytes32 indexed deviceIDHash, bytes32 indexed userIDHash, string resource,
string reason);
modifier onlyApprovedDevice(bytes32 _deviceIDHash) {
require(registeredDevices[_deviceIDHash].approved, "Device not approved.");
_;
}
modifier onlyActiveUser(bytes32 _userIDHash) {
require(registeredUsers[_userIDHash].active, "User not active.");
_;
}
// Function to register a new device onto the blockchain
function registerDevice(bytes32 _deviceIDHash, string memory _deviceType, string memory
_securityZone) public returns (bool) {
require(registeredDevices[_deviceIDHash].deviceIDHash == 0, "Device already registered.");
registeredDevices[_deviceIDHash] = Device(_deviceIDHash, msg.sender, _deviceType,
_securityZone, true);
emit DeviceRegistered(_deviceIDHash, _deviceType);
return true;
```



```
}
// Function for a user to request access to a network resource
function requestAccess(bytes32 _userIDHash, bytes32 _deviceIDHash, string memory _resource)
public onlyApprovedDevice(_deviceIDHash) onlyActiveUser(_userIDHash) returns (bool) {
// Complex access logic here: based on user role, device type, security zone, resource sensitivity
// Example: Only "Admin" role from "Internal" zone can access "CriticalServer_DB"
string memory userRole = registeredUsers[_userIDHash].role;
string memory deviceZone = registeredDevices[_deviceIDHash].securityZone;
if (keccak256(abi.encodePacked(userRole)) == keccak256(abi.encodePacked("Admin")) &&
keccak256(abi.encodePacked(deviceZone)) == keccak256(abi.encodePacked("Internal")) &&
keccak256(abi.encodePacked(_resource)) == keccak256(abi.encodePacked("CriticalServer_DB")))
{
// Log successful access
// authorizedAccesses[_deviceIDHash].push(_userIDHash); // Not strictly necessary to store on-chain
for every access
emit AccessGranted(_deviceIDHash, _userIDHash, _resource);
return true;
} else {
emit AccessDenied(_deviceIDHash, _userIDHash, _resource, "Policy violation.");
return false;
}
}
//... other functions for user registration, deactivation, policy updates...
}
```

How It Works

Each device (IoT sensor, laptop, server) and user has a unique cryptographic identity registered on the blockchain. When a device or user attempts to connect or access a resource, network agents (or integrated network devices) call the requestAccess function on the smart contract. The contract, based on predefined immutable rules, verifies identity, role, and permissions against the distributed ledger. The outcome (access granted/denied) is recorded on the blockchain as an immutable event, providing a transparent audit trail.

CONCLUSION

The extensive journey through the conceptualization and modeling of a blockchain-secured LAN reveals a landscape of profound transformation. We conclude that the integration of blockchain technology moves the security paradigm from a static, reactive stance to a dynamic, proactive state of continuous consensus. The proposed framework successfully addresses critical flaws in the traditional model: it eliminates single points of failure, provides an immutable and transparent audit trail for all network events, and automates enforcement through tamper-proof smart contracts, thereby significantly reducing the attack surface and the potential for human error or malicious insider threat.

However, this vision is not without its frontiers. The challenges of computational overhead, network latency introduced by consensus mechanisms, and the initial complexity of deployment are non-trivial and demand further research into lightweight consensus protocols and hardware integration. This work is not a call for the immediate dismantling of existing security infrastructure, but rather a foundational argument for its inevitable evolution.

Ultimately, the most significant implication of this research is philosophical. It demonstrates that trust in a network need not be vested in a central authority, but can be distributed, earned through verification, and embedded into the very fabric of the system. The future of LAN security lies not in building higher walls, but in weaving a stronger, smarter web – one where every thread validates every other. This blockchain-based model provides the blueprint for such a web, promising a new era of resilience where security is not a feature added to the network, but the defining characteristic of the network itself.

REFERENCES

1. Govea J, Gaibor-Naranjo W, Villegas-Ch W. Securing critical infrastructure with blockchain technology: An approach to cyber-resilience. Computers. 2024 May 15;13(5):122.
2. Saleh AM. Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. Blockchain Res Appl. 2024 Sep 1;5(3):100193.
3. Hanumantharaju R, Shreenath KN, Sowmya BJ, Supreeth S, Shruthi G, Rohith S, et al. Blockchain-based machine learning approach for secure and efficient vehicular data monitoring and analysis. Discov Comput. 2025 Nov 7;28(1):259.
4. Almarri S, Aljughaiman A. Blockchain technology for IoT security and trust: A comprehensive SLR. Sustainability. 2024 Nov 21;16(23):10177.
5. Liyakat KK, Halli UM. Nanotechnology in IoT security. J Nanosci Nanoeng Appl. 2022;12(3):11–16.
6. Akansha K. Email security. J Image Process Intell Remote Sens. 2022 Oct;2(6):295–320.
7. Pol RS, Deshmukh AB, Jadhav MM, Liyakat KK, Mulani AO. I-button based physical access authorization and security system. J Algebraic Stat. 2022 May 1;13(3).
8. Kutubuddin K. Blockchain-enabled IoT environment to embedded system: A self-secure firmware model. J Telecommun Stud. 2023;8(1).
9. Chinthamu N, Prasad M, Chinchawade AJ, Liyakat KK, Deepti K, Karukuri M, et al. Self-secure firmware model for blockchain-enabled IoT environment to embedded system. Eur Chem Bull. 2023;12(S3).
10. Gund VD. PIR sensor-based Arduino home security system. J Instrum Innov Sci. 2023;8(3):33–37.
11. Liyakat KK. Implementation of e-mail security with three layers of authentication. J Oper Syst Dev Trends. 2022;9(2):29–35.
12. Torii N, Yamamoto D, Matsumoto T. Evaluation of latch-based physical random number generator implementation on 40 nm ASICs. In: Proceedings of the Trustworthy Embedded Devices Workshop. 1st ed. New York (NY): ACM; 2016. p. 23–30.

