

Blockchain, AI and Decentralized Identity for Edge Computing

Dr X Catherine Arputha Divya

Assistant Professor

Department of Commerce CA & BA

Sri Krishna Arts And Science College, CBE

Mail ID : kathu777@gmail.com

Abstract

The proliferation of Internet of Things (IoT) devices necessitates a shift from traditional centralized cloud processing to distributed network architectures, leading to the creation of Edge of Things (EoT) networks. While Edge Computing effectively reduces latency and computational burdens for time-sensitive applications like smart healthcare and smart transportation, its distributed nature introduces significant challenges regarding security, privacy, and identity management. This paper explores the critical convergence of Blockchain, Artificial Intelligence (AI), and Decentralized Identity (DI) to establish secure, scalable, and trustworthy systems for edge computing environments. Blockchain provides decentralization, immutability, and traceability, addressing vulnerabilities inherent in EoT systems. Decentralized Identity (DI), specifically Self-Sovereign Identity (SSI), restores user control over verifiable credentials (VCs) and Decentralized Identifiers (DIDs), creating a foundation of verifiable trust. Furthermore, AI offers the necessary intelligence for advanced fraud detection, autonomous decision-making, and process optimization within these complex, latency-sensitive infrastructures. This integrated approach not only enhances performance but also prepares the ecosystem for future threats, such as those posed by quantum computing, through solutions like Quantum Key Distribution (QKD).

Keywords: Artificial Intelligence (AI), Block Chain, Decentralized Identity (DI), Quantum Key Distribution (QKD).

I. Introduction

The rapid expansion of IoT devices, predicted to surpass 500 million connected devices by 2030, drives the demand for computational resources that can handle massive data streams with low latency requirements. Edge Computing addresses this need by migrating processing and storage to the network edge, giving rise to the Edge of Things (EoT) paradigm. EoT environments enable time-sensitive service delivery by minimizing communication overhead and latency, typically reducing round-trip time (RTT) from 50–200 milliseconds (ms) to single-digit or sub-millisecond latency for critical processing tasks. Applications in autonomous vehicles, industrial IoT (IIoT), and remote healthcare rely on this ultra-low latency for real-time control and decision-making.

However, this decentralization exposes the network to new security and privacy threats, including Distributed Denial-of-Service (DDoS) attacks, data breaches, and unauthorized modifications. The core challenge lies in building a trust infrastructure that is distributed, verifiable, and capable of operating autonomously at the edge.

The integration of Blockchain technology, forming the Blockchain-enabled Edge of Things (BEoT) paradigm, offers fundamental security properties such as decentralization, immutability, and traceability to counter these threats. Furthermore, Decentralized Identity (DI) using SSI principles, coupled with Artificial Intelligence (AI), provides the crucial layers of user control, data provenance, and automated intelligence necessary for the next generation of digital trust.

Review of Literature:

Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications by tri ngugen, journal of network and computer applications, these systems still have limitations, such as lack of security, high latency, energy inefficiency, the inefficiency of bandwidth utilization, and shortage of automaticity. The integration of edge computing and blockchain into IoT has been proposed to address these limitations. Yet, this integration is challenging and has not been deeply investigated. This paper aims to conduct a review of the integration of edge computing and blockchain into IoT systems. To the best of our knowledge, this is the first review paper that covers all

aspects of system architectures and categories of blockchain-based edge deployment, complete security requirements, including confidentiality, integrity, authentication, authorization/access control, privacy, trust/confidence, transparency, availability, secure automaticity, and tolerance, and applications of blockchain-based edge potential usages with consideration of security requirements. Additionally, this review provides comprehensive discussions of challenges and insights into the future direction of blockchain-based edge IoT systems.

Blockchain and edge computing technology enabling organic agricultural supply chain: A framework solution to trust crisis by sensen hu, computers and industrial engeering , volume 153, march 2021

In this paper, we first leverage the immutability of blockchain and the paradigm of edge computing to construct an OASC's trust framework, which has a much better trade-off between cost and efficiency. Further, according to the scenarios of OASC, we divide all the stakeholders into four roles, proposing a novel consensus mechanism to manage the information flow. The evaluation results demonstrate that our proposal can significantly achieve the performance improvement as well as the cost decline compared to the traditional approach. This framework will also make affordable traceability solutions for those in developing countries at a low cost in the future.

II. The Edge Computing and Blockchain Foundation (BEoT)

A. Edge Computing and the EoT Architecture

Edge computing integrates with IoT networks to form the EoT, serving as computation nodes placed near the end-user, often at access points or base stations. Edge Servers (ESs) are equipped with rich resources to handle data tasks, providing services ranging from data analytics to prediction and storage. This location-aware, distributed processing eliminates the computational burden on resource-constrained IoT sensors and ensures low-latency response, vital for industrial and smart city applications.

A generic BEoT architecture consists of three core entities: IoT (devices generating data), Edge Computing (ESs performing local processing), and the Blockchain Network (interconnecting entities in a decentralized fashion). In this convergence, ESs can function as blockchain miners, verifying transactions and producing data blocks to maintain the network.

B. Blockchain for Security and Trust

Blockchain enhances security in edge networks by providing unique properties that overcome the single point of failure and centralized control issues of conventional systems. The immutability and consensus mechanisms of blockchain guarantee the reliability and trustworthiness of information transferred over the network. Key security services supported by BEoT include access authentication, data privacy preservation, attack detection, and trust management.

For example, in smart transportation systems, blockchain manages secure data analytic services at edge vehicular servers (e.g., roadside units) to support fast traffic control and reliable vehicle routing, even in untrusted environments. Similarly, in smart grids, blockchain ensures secure and privacy-preserving energy trading transactions.

III. Decentralized Identity (DI) and AI Convergence

A. Self-Sovereign Identity (SSI) in Edge Computing

Self-Sovereign Identity (SSI) fundamentally shifts control over identity data from centralized authorities to the user or entity, which aligns perfectly with the decentralized nature of edge networks. This paradigm relies on core technical components:

1. **Decentralized Identifiers (DIDs):** DIDs are unique, global identifiers that are cryptographically verifiable and resolvable. Unlike traditional IDs, DIDs are controlled by the user, providing security and autonomy. DIDs are anchored on decentralized networks like blockchains and resolve to a DID Document containing public keys and service endpoints.

2. **Verifiable Credentials (VCs):** VCs are tamper-evident, digitally signed statements issued by a trusted authority (the Issuer), confirming specific attributes about the identity (the Holder). VCs enable cryptographic verification without continuous reliance on the original issuer.
3. **Zero-Knowledge Proofs (ZKPs):** ZKPs allow a user to prove a statement is true (e.g., being over 18) without revealing any underlying sensitive data, supporting privacy-preserving identity systems via selective disclosure.

The integration of DIDs and VCs into the IoT lifecycle, termed DIAM-IoT, enables a unified, interoperable, and tamper-proof device identity registry managed on the blockchain, granting device owners full control over their data access. For autonomous AI Agents, SSI provides Non-Human Identities (NHIs) via DIDs and VCs, explicitly detailing the agent's roles, permissions, and authorizations, which is critical for accountability in multi-agent environments.

B. The Role of AI in Enhancing Verifiable Trust

AI introduces intelligence and automation to SSI systems. SSI provides AI systems with trustworthy, provenance-rich, user-authorized inputs, which AI then processes to automate decisions, verify credentials, and detect fraud more efficiently.

1. **Verification and Fraud Detection:** Machine learning algorithms can efficiently validate VCs by detecting anomalies and subtle behavioral patterns, strengthening fraud detection beyond traditional rule-based systems.
2. **Explainable AI (XAI):** XAI is a crucial complement, ensuring that algorithmic decisions in high-stakes environments like identity management are transparent and interpretable. Integrating XAI with SSI means systems can provide clear justifications when a credential is rejected, strengthening accountability and user trust.
3. **Privacy-Preserving Training:** Traditional AI often relies on centralized data, conflicting with SSI principles. **Federated learning** allows models to be trained across multiple devices using SSI-verified data, sharing only model updates instead of raw sensitive data, thus aligning AI performance with privacy requirements like GDPR.

IV. Specialized Applications in Edge Environments

The BIoT paradigm unlocks new industrial and customer applications by offering enhanced security and speed across diverse domains.

A. Smart Transportation

Smart transportation relies on fast data processing for time-sensitive services such as reliable vehicular management and low-latency traffic control. Deployments utilize edge nodes (like roadside units) forming sub-blockchain networks to manage large volumes of traffic data, overcoming the challenge of centralized server failures. The combination of BIoT ensures increased network performance with reduced latency and employs smart contracts for secure transactions, such as payment purposes in platoon driving models for autonomous vehicles.

B. Smart Healthcare

In remote healthcare (telehealth), decentralized Identity Management (IdM) is essential due to the sensitive nature of patient data. Centralized legacy IdM systems create data silos, lack interoperability, and force patients to trust service providers completely. The proposed *Health-ID* framework uses a consortium Ethereum blockchain managed by healthcare regulators to tokenize patient and provider identities (healthID), enabling transparent and secure authentication across different eHealth domains. Edge computing supports faster patient data processing with reduced latency. Access control for electronic health records (EHR) can be provided using a hybrid blockchain-edge architecture where access events are verified via a mutual agreement mechanism before being included in the blockchain.

C. Smart City and IIoT

Smart City applications leverage BIoT for secure services, encompassing areas like smart grid, smart home, and smart surveillance. Blockchain frameworks enable secured and transparent data-sharing among users across multiple trust domains. Cognitive edge nodes in smart city infrastructure utilize AI algorithms for mining data, allowing early prediction of structural health problems in buildings (SHM) or assisting in real-time video analysis for surveillance, with smart contracts managing decisions and sharing immutable records. In Industrial IoT (IIoT), edge computing combined with DI is crucial for secure device onboarding, data transmission, and access control for resource-constrained devices, often leveraging specialized protocols like Hyperledger Indy and DIDs.

V. Security Challenges and Quantum Future

A. Resource Constraints and Scalability

Despite the benefits, implementing blockchain on resource-constrained Edge Servers (ESs) and IoT devices presents significant challenges. Issues include:

1. **High Latency:** The requirement for block synchronization and consensus mechanisms inherently introduces delays, which can inhibit Spatio-temporal sensitive applications like mobile self-driving vehicles.
2. **Storage Overhead:** The blockchain distributed ledger requires significant storage, leading to scalability issues as the chain grows, making it difficult for resource-constrained IoT devices to store full ledgers.
3. **Energy Consumption:** Running computationally intensive consensus algorithms like Proof of Work (PoW) results in extensive energy consumption and high network latency.

Solutions often involve using lightweight consensus protocols, applying sidechains or Layer-2 technologies to handle large data streams off-chain, and segregating metadata required for blocks to reduce storage overhead. The feasibility of implementations like the Health-ID scheme on consortium blockchains shows high throughput (over 100 TPS) can be achieved by optimizing parameters like block-time and minimizing the number of sealers.

B. Quantum Uncertainty and Mitigation

A profound threat to current cryptographic security in edge computing arises from the future potential of quantum computing. Quantum algorithms, such as Shor's and Grover's, make it easy to break the cryptographic keys used by classical algorithms (like ECC, RSA, and Diffie-Hellman) for device authentication and encryption, rendering existing systems vulnerable.

To address this, a "Blockchain-based Device Authentication in Edge Computing Using Quantum Approach" (BDAEC-QA) has been proposed, which uses **Quantum Key Distribution (QKD)**, context information, and blockchain to provide secure authentication for IoT devices. Globally, standardization bodies are preparing for post-quantum cryptographic standards (NIST PQC) to ensure the long-term resilience of identity systems. Hybrid trust architectures that combine classical and quantum-resistant primitives are necessary to mitigate systemic risks.

How it Works:

- **Decentralized Identity (DID):** Users and devices have self-sovereign identities, creating, owning, and managing their digital credentials without relying on a central authority.
- **Verifiable Credentials:** Identity data is stored in decentralized wallets, and verifiable credentials are issued and verified instantly and securely.
- **Blockchain as a Ledger:** The blockchain serves as a tamper-proof ledger, recording transactions and ensuring the integrity and immutability of identity data.
- **Smart Contracts:** Smart contracts automate access control and credential management, defining permissions and enabling secure, trustless interactions.

- **Zero-Knowledge Proofs (ZKPs):** These cryptographic techniques allow for selective disclosure of information, enabling users to prove their identity or attributes without revealing unnecessary personal details.

Benefits for Edge Computing:

- **Enhanced Security:** Eliminates single points of failure inherent in centralized systems, protecting against data breaches and unauthorized access.
- **User Control & Privacy:** Individuals and devices maintain sovereignty over their identity data, deciding who can access it and under what conditions.
- **Trust and Transparency:** The distributed ledger and consensus mechanisms ensure transparency and provide a verifiable, tamper-proof record of identity events.
- **Interoperability:** Enables secure communication and transaction between edge devices without needing a central intermediary.
- **Scalability:** By integrating with decentralized file systems like IPFS, these systems can improve performance and scalability for large-scale edge deployments.

Challenges:

- **Scalability:** The rapid expansion of IoT ecosystems presents challenges for the scalability of blockchain in edge computing.
- **Performance and Latency:** The inherent latency of blockchain systems can impact the real-time performance required for some edge applications.
- **Complexity:** Developing and implementing these complex systems requires advanced expertise in blockchain, cryptography, and edge computing.

VI. Conclusion

The integration of Blockchain, AI, and Decentralized Identity marks a foundational shift in addressing the security and privacy challenges inherent in distributed Edge Computing environments. Blockchain provides the core trust layer via immutability and decentralization, mitigating threats like single points of failure and malicious data injection. SSI leverages this foundation to empower users and autonomous AI agents with verifiable, user-controlled identities (DIDs and VCs). AI enhances this framework by providing the analytical capabilities for real-time fraud detection (ML), transparency (XAI), and optimized privacy-preserving processing (federated learning). While challenges related to latency, storage, and energy efficiency persist, targeted architectural solutions, including consortium blockchains and optimized cryptography, demonstrate pathways toward scalable and high-performing BIoT environments. Crucially, anticipating quantum threats with solutions like QKD and post-quantum standards ensures the longevity and cryptographic resilience of this emerging Global Trust Infrastructure.

The future of edge computing is defined by this convergence, moving beyond mere connectivity to establishing a reliable, auditable, and human-centric digital society where trust is a computable property. This holistic architecture ensures that technology acts as a tool of liberation, safeguarding individual autonomy and accountability in an increasingly automated and interconnected world.

Reference

1. <https://www.sciencedirect.com/science/article/abs/pii/S1574013724000510>
2. <https://www.mdpi.com/1999-5903/17/1/45>
3. <https://www.embedded.com/embedding-blockchain-for-enhanced-security-in-iiot-networks/>
4. https://www.researchgate.net/publication/349469626_Embedding_Blockchain_Technology_Into_IoT_for_Security_A_Survey

5. Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications by tri ngugen, journal of network and computer applications, volume 226, June 2024
6. Blockchain and edge computing technology enabling organic agricultural supply chain: A framework solution to trust crisis by sensen hu, computers and industrial engeering , volume 153, march 2021