

Securing the Decentralized Future: A Comprehensive Survey of Blockchain-Integrated Architectures for Identity, Privacy, and Access Control in Multi-Domain Systems

Rupsingh Puransingh Mathwale

Department of Information Technology
SGGS Institute of Engineering and Technology Nanded 431606
Maharashtra, India

Ankush D. Sawarkar

Department of Information Technology
SGGS Institute of Engineering and Technology Nanded 431606
Maharashtra, India

ABSTRACT

Internet of Things (IoT) devices are increasingly integrated into smart infrastructures, making security, privacy, and access control critical concerns. It is inevitable but to consider confidentiality, Integrity and Availability of IoT devices. There are several security vulnerabilities with the traditional centralized architectures, i.e. single point of failure and concentrated threat surface. Blockchain technology addresses the security challenges posed by centralized architecture. Blockchain is a distributed ledger technology which records transactions taking place on the network. Bitcoin is the proven application of blockchain technology. Blockchain is an immutable, add only ledger of blocks of transactions. This secure and resilient aspect of blockchain could be utilized in various non cryptocurrency applications as well. This survey provides a thorough analysis of blockchain applications across various domains, including healthcare (Internet of Medical Things [IoMT]) for securing clinical data and vehicular networks (Internet of Vehicles [IoV]) for reliable message transfer. Blockchain could significantly affect the way in which Identity and access Management works through adaptation of Self Sovereign Identity (SSI) and Decentralized Identifiers (DID), which shifts the control of the identity data at user end, and it could be used in Know Your Customer(eKYC) processes as well. For network resource management, blockchain integrates seamlessly with federated learning, 5G, and metaverse platforms. Despite these benefits, scalability limitations and transaction latency remain major concerns in blockchain-based solutions. In addition to multi-domain applications, the paper examines decentralized authentication paradigms, Zero Trust Architectures (ZTA), and post-quantum privacy-preserving primitives. By mitigating domain specific issues, Blockchain technology could act as a promising tool in securing decentralized systems.

General Terms

Security, Authentication, Privacy

Keywords

Blockchain, IoT, Privacy, Security, Access Control

1. INTRODUCTION

The Internet of Things (IoT) will become an essential part of the modern-day global infrastructure that networks everything from human wearable smart devices to critical industry sensors. Current computations indicate that the worldwide base of connected devices has already surpassed previous projections, resulting in an unprecedented amount of data that must be processed in real time and kept secure [1]. This huge connectivity spurs the innovation of smart services, but it also increases the digital attack surface which threatens the confidentiality, integrity, and availability (CIA) of data. Decentralized architectures are multi-party protocols that do not rely on trusted third parties to eliminate single points of failure, and more generally, put greater distance between malicious attacks and a loss of security function. As a decentralized base, blockchain technology has been developed to deal with such security loopholes. Initially designed for peer-to-peer financial transactions, its core features of immutability, transparency, and cryptographic auditability today provide a robust basis for secure data exchange without central intermediaries. The distributed consensus protocols and smart contracts enable interactions among heterogeneous IoT entities in an automated and tamper-proof manner through blockchain ledger. Blockchain technology is transforming many significant industries. In healthcare, IoMT [2] has been using distributed ledger technology to secure Electronic Health Records (EHRs) [3] from hackers, in addition to ensuring seamless data exchange between authorized parties. The use of blockchain technology in transportation ensures anonymous authentication [4] and intrusion detection for IoV [5] and UAVs [6] to protect them from any possible cyber threats that could pose physical harm. The research continues to show a gap in scalability, where the growth of transactions causes performance issues in throughput and latency. These limitations, together with the need for interoperability and resistance to quantum [7] computing attacks, are still an area of research. Distinct from prior survey literature, the present study examines decentralized identity management, smart-contract-based access control, Zero Trust Architectures [8], and post-quantum cryptographic defense through blockchain.

This survey is organized as follows so that we can give a comprehensive analysis of this evolving field. Section II presents the basic concepts of blockchain technology and its integration with IoT architecture. In the Section III, we discuss domain-specific applications including health care, intelligent transportation systems, and smart cities. In Section IV, we discuss existing decentralized identity and access control systems such as Self Sovereign Identity (SSI) [9] and e-Know Your Customer (eKYC) [10] methods. Prior studies [11] have provided risk management strategies in blockchain based identity management systems. Section V discusses security services and cyber defense mechanisms including intrusion detection and Block chained Federated Learning [12]. Section VI addresses technical difficulties, particularly related to scalability, resource constraints, and interoperability [13]. Section VII covers future work possibilities like Post-Quantum Security and Zero Trust Architectures, further zero knowledge proofs can be used for fraud detection and achieving transparency [14], and Section VIII gives conclusions.

The remainder of this survey is structured to provide an exhaustive architectural evaluation: Section II provides blockchain fundamentals and IoT interfacing mechanisms; Section III gives details about domain-specific implementations across healthcare, intelligent vehicular systems, and smart municipalities; Section IV discusses decentralized identity models (SSI/DIDs) and access control schemes; Section V provides details about cyber defense mechanisms, including collaborative intrusion detection and federated learning; Section VI identifies scalability bottlenecks and resource constraints; Section VII discusses post-quantum cryptography and Zero Trust integration; and Section VIII concludes the study.

2. FUNDAMENTALS

2.1 Blockchain Fundamentals

Blockchain could be defined as an increasing sequence of blocks, blocks in turn are a collection of transactions, each block is linked to the previous block by hashing mechanism, thereby creating a tamper proof chain of transactions. By making use of cryptography trust and consensus is provided in an untrusted world. Blockchain technology has evolved over the years through the following five generations:

Blockchain 1.0 (Cryptocurrency): The first cryptocurrency Bitcoin [15] was developed as a peer-to-peer virtual currency using cryptography without involvement of any trusted third-party authority like a Bank or Government.

Blockchain 2.0 (Smart Contracts): Blockchain frameworks like Ethereum [16] were developed to provide programmable and customizable blockchain, which provided an option to customize blockchain as required by the target application instead of tightly binding to any single application like cryptocurrency.

Blockchain 3.0 (Interoperability): Network systems like Polkadot [17] allowed heterogeneous blockchains to communicate with each other and leverage their advantages.

Blockchain 4.0 (Interfacing with Enterprise): Frameworks like Hyperledger Fabric [18] allowed integration of collaborated blockchain systems with existing applications.

Blockchain 5.0 (AI Integration): AI integration automated smart contract optimization and increased overall security in self-optimizing fashion [19].

2.1.1 Key Features of Blockchain. **Immutability:** It is totally infeasible to tamper data present in blocks; this is due to linked blocks by hashes. If a block's data is to be tampered then all the blocks af-

ter this block must be updated, that is computationally infeasible. **Transparency:** All the blocks are updated with same data across multiple locations resulting in transparency of operations which could be useful in multiple governance applications

Consistency: Data in all the distributed ledgers across multiple locations is kept in synchronization by means of consensus algorithms. consensus is the decision, which will be followed for updating the ledger.

Availability: Due to replication of blockchain ledgers across multiple locations, availability of data is ensured, which results in uninterrupted supply of the requested data to the legitimate user.

Table 1 illustrates Comparison of Public, Private, and Consortium Blockchains.

Table 1. Comparison of Public, Private, and Consortium Blockchains

Feature	Public	Private	Consortium	Ref.
Identity	Anonymous / Pseudonymous	Pre-approved / Known	Pre-approved / Authorized	[10, 11]
Access Control	Open to all	Restricted to one organization	Shared among multiple entities	[20]
Trust Level	Low (Trustless)	High (Trusted nodes)	Medium (Pre-verified nodes)	[8, 21]
Consensus	All nodes	Single organization	Multiple organizations	[1, 22]
Throughput	Low	Very High	High	[1, 22]
Examples	Bitcoin, Ethereum	Quorum	Hyperledger Fabric	[15, 16, 18, 23]

2.2 IoT Interfacing: The BCIoT Framework

Traditional centralized IoT systems, especially in IoMT, IoV and other critical applications can pose serious security threats:

Center for Data Breaches: The centralized system can motivate the attackers to concentrate on the single system to bring down all the ongoing critical operations.

High Latency: All the data must go and come back from a single entity creating network congestion and further creating vulnerability.

Scalability: With a centralized system there is limitation of scalability on the number of end devices interfaced with it. Blockchain based IoT overcomes the limitations with the centralized IoT systems.

Data Integrity: Data in BCIoT is securely distributed across multiple locations, eliminating the single point of failure and single point of attack issue with centralized systems.

Low Latency: For transactions data from the distributed blockchain ledgers can be accessed, so overall access time gets reduced drastically.

Scalability: Due to separate ledgers and decentralized control some aspects of scalability can be addressed. BCIoT system architecture for vehicle networks can be illustrated with four layers [1, 21]. Figure 1 illustrates Layered Architecture of blockchain based system

Physical Layer: It contains end devices i.e. sensed e vehicles
Network/Management Layer: Controlled by Network Control Centers (NCC). The role of NCC is to register the users and provide

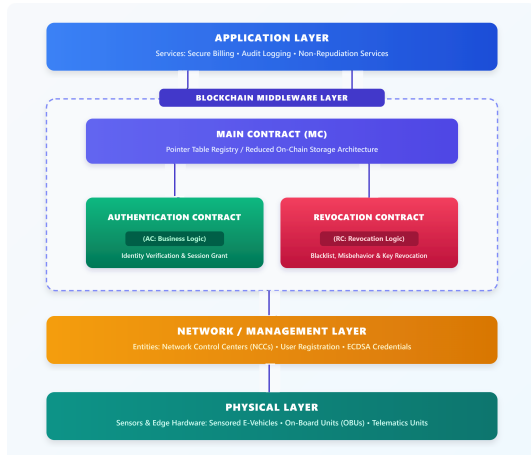


Fig. 1. Layered Architecture of blockchain based system

ECDSA credentials.

Blockchain Middleware Layer: Nodes with a special smart contract interaction pattern.

Main Contract (MC): Acts as a pointer/mapping table that stores the address of the Authentication Contract (AC) and others to reduce storage space.

Authentication Contract (AC): The business logic of smart contracts for verification of authentication data.

Revocation Contract (RC): It contains logic related to revocation of access through smart contracts.

Application Layer: Used to ensure nonrepudiation, for example in billing process.

2.3 Comparative Analysis

The consensus protocol dictates the mechanism in which blocks can be appended to the blockchain ledger. The consensus protocols can be compared over the aspects like energy consumption, scalability and application suitability. Table 2 compares Proof of Work, Proof of Stake, Practical Byzantine Fault Tolerance, Delegated Proof of Stake and Proof of Elapsed Time consensus algorithms. Table 3 compares traditional IoT with BCIoT.

Table 2. Consensus Algorithms for IoT

Alg.	Key Feature	Energy	Scale	IoT Suitability	Ref.
PoW	Complex puzzles	Very High	Low	Resource-heavy	[24]
PoS	Coin stake	Low	Med.	Higher throughput	[25]
PBFT	Voting-based	Low	Low	Private networks	[26]
DPoS	Delegates	Low	High	Fast and efficient	[27]
PoET	TEE wait time	Very Low	High	IoT-friendly	[28]

Table 3. Centralized IoT vs. BCIoT

Metric	Centralized IoT	Blockchain IoT
Architecture	Client-Server	Peer-to-Peer (P2P)
Trust Model	Trusted Third Party (TTP)	Trustless
Security	Single Point of Failure	Fault Tolerant
Data Integrity	Server-side Tampering Risk	Immutable Records
Operating Cost	High Maintenance Cost	Lower Cost

3. MULTI-DOMAIN APPLICATIONS OF BCIOT

The Internet of Things and blockchain technology help solve problems related to security and privacy with the Internet of Things. The Internet of Things and blockchain technology are a team because blockchain technology keeps a record of everything that happens and this record cannot be changed. This makes the Internet of Things more private. This section looks at the main application areas: Healthcare (IoMT), Intelligent Transportation Systems (ITS/IoV), and Smart Cities.

3.1 Healthcare and the Internet of Medical Things (IoMT)

IoMT uses sensors and wearable technologies to allow for remote monitoring of vital health information such as heart rates and oxygen levels of patients. Some of the critical healthcare services which can be facilitated using blockchain technology include: Management of Electronic Health Records (EHRs): Existing management frameworks for EHRs experience problems related to interoperability and data silos. By using blockchain technology, EHRs can be shared among different facilities in a secure manner and ensure data integrity. The use of a framework such as MedRec [29] makes this possible by leveraging Ethereum-based smart contracts to manage permission to access data. Remote Patient Monitoring: In the case where remote patient monitoring is necessary in aged populations, especially those living with diseases like diabetes, blockchain guarantees data integrity when transferring the data from IoT devices to healthcare organizations. Technologies such as Healthchain [30] have been used in this regard.

3.2 Intelligent Transportation Systems (ITS) and Vehicular Systems

Vehicles to everything communication are critical for transportation systems. It helps make the roads safer and traffic flow better. The main goal of vehicles for communication is to improve security on the roads and make traffic more efficient. This is what vehicle to everything communication is. Blockchain tackles the problem of vulnerabilities in the open wireless environment of vehicular ad-hoc networks.

Secure Authentication and Privacy: To protect against attacks such as impersonation and Sybil attacks, some of the blockchain-based authentication mechanisms (like BARM, DBCPA [31]) offer conditional anonymity that enables anonymous authentication with the help of pseudonyms.

Accidents Forensics and Notification: The BCAS-VADN [32] system enables the reporting of accidents in a blockchain-secured manner. Such accidents are reported to emergency services and can no longer be altered since the information will be recorded immutably.

Internet of Drones (IoD) : Blockchain has been applied to UAV net-

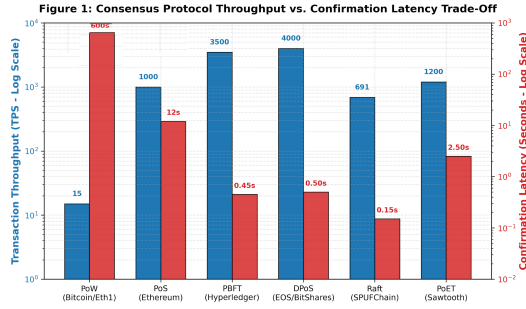


Fig. 2. Self Sovereign Identity trust triangle

works, enabling secure navigation and air traffic management and data dissemination from drones involved in surveillance or medical transport missions [33].

Incentives: On the Internet of Vehicles (IoV), tokenization of the IoV's shared resources such as energy or data is achieved through blockchain, allowing drivers to gain energy coins for sharing idle energy resources with the network.

As illustrated in Figure 2, selecting a consensus mechanism for BCIoT requires balancing transaction throughput vs latency. While Proof-of-Work (PoW) achieves decentralization with high latency (~6000s) and low throughput (~15 TPS), permissioned mechanisms like PBFT and Raft provide confirmation (~0.5s) and high throughput (~1,000 TPS). This makes voting-based consensus essential for latency-centric vehicular (IoV) and healthcare (IoMT) applications, despite $O(N^2)$ message complexity limiting scale to $N < 50$ validation nodes.

3.3 Smart Cities and Open Systems

Smart Cities [34], use different IoT sensors to control urban facilities such as energy, waste management, and public security. Decentralized Public Services: Blockchain provides Blockchain-as-a-Service (BaaS), which offers a solution for municipalities to offer services related to smart homes, healthcare, and transportation. BaaS can assist municipalities in eliminating Single Points of Failure (SPOF) in huge city networks.

Decentralized Energy Grid: Using blockchain technology allows creating decentralized energy datahubs to enable Peer-to-Peer (P2P) energy exchange. Users will be able to exchange energy within their neighborhoods. Smart contracts help automate energy exchange and billing processes using platforms such as Energy Web Chain. Decentralized Smart Homes: The examples of blockchain-based smart home architecture include SHIB [35] technologies that ensure secure communication between devices and prevent personal information leakage by the user.

Data Marketplace: Technologies like Databroker, Datapace [37] have developed distributed marketplaces for trading of IoT sensor data in a secure way. Table 4 illustrates Comparison of Blockchain Applications in IoT Domains.

4. DECENTRALIZED IDENTITY AND ACCESS CONTROL SYSTEMS

4.1 Smart Cities and Public Infrastructure

SSI, or Self-sovereign Identity, represents a novel approach to identity management, moving from systems managed by third-party providers to a user-controlled model in which the user fully owns

Table 4. Blockchain Applications in IoT

Domain	Use Cases	Benefit	Frame-works	Ref.
Healthcare	EHR sharing, remote monitoring	Data integrity, patient privacy	MedRec	[3, 29]
Transportation	V2X security, drone navigation	Authentication, non-repudiation	BARM, DBCPA	[4, 32, 34]
Smart Homes	Automation, security monitoring	Data sovereignty, access control	SHIB	[35]
Smart Cities	Smart grids, public safety	Decentralization, no SPOF	Privy-Sharing	[33, 36]

and controls their digital identities, managing all attributes independently without relying on third party intermediaries. SSI technology is based on the "trust triangle" which involves three main parties:

Issuer – subject issuing credentials for the Holder. Holder – a subject possessing his/her digital wallet. Verifier – a subject that verifies credentials. As for the underlying technologies of SSI, there are two main concepts:

Decentralized Identifiers (DID); Verifiable Credentials (VC).

Decentralized Identifiers (DID): Did refers to a publicly accessible URI associated with a particular subject and stored as part of a DID document which is in a verifiable data registry (usually a blockchain). A DID controller can prove its possession independently of a centralized certificate registry.

Verifiable Credentials (VC): A Verifiable Credential (VC) can be referred to as a digital form of a physical credential such as diplomas or licenses. The credential contains some specific claims (attributes) and is signed by the issuer's private key with its public key stored in the blockchain, which can be used for verification. Figure 4 illustrates the Self Sovereign Identity trust triangle.

4.2 Blockchain-Enabled Electronic Know Your Customer (eKYC)

The conventional KYC process has been seen to be uneasy for customers, time-consuming, repetitive, and associated with errors by its dependence on manual paperwork and centralized management. The advent of electronic KYC (eKYC) has brought a new approach that involves digitization and biometric identification of the individual. Blockchain integration enhances the efficacy of eKYC [38] by creating an open and tamper-resistant trust system. One of the benefits of using blockchain technology in electronic KYC includes the use of the "verify once, share many" method. This is because when one's identity is verified by an organization such as the bank, their information is stored in the blockchain, making the task simpler when requesting another service from another entity since all that it requires is a quick check of the blockchain database to authenticate the person's identity. Smart contracts ensure this task is automated and done with the users' agreement.

Resource-constrained IoT edge devices exhibit severe performance bottlenecks under complex cryptographic operations. As shown in Figure 3, executing a bilinear pairing ($T_{bp} \approx 32.1$ ms) on an IoT edge node (e.g., Raspberry Pi 3) incurs over $14\times$ the execution delay of Elliptic Curve scalar multiplication ($T_{ecm} \approx 2.3$ ms) and $100\times$ that of SHA-256 hashing ($T_h \approx 0.31$ ms). To prevent authentication queues during peak network traffic, BCIoT frame-

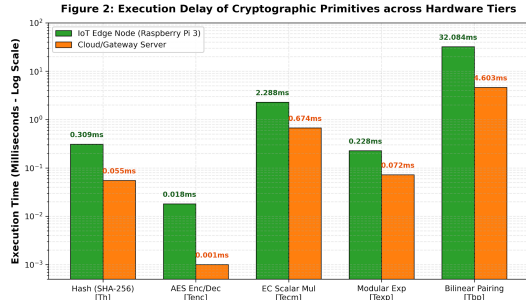


Fig. 3. Execution Delay of Cryptographic Primitives across Hardware Tiers

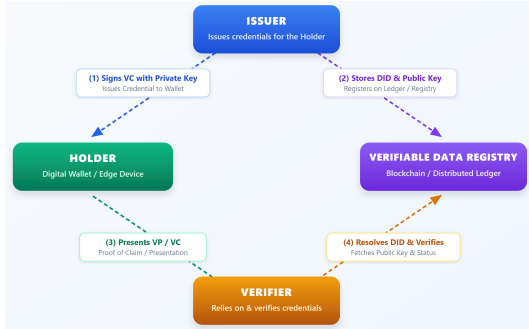


Fig. 4. Self Sovereign Identity trust triangle

works must utilize pairing-free ECDSA schemes paired with off-chain hash pointer contracts.

4.3 Decentralized Access Control Systems

Blockchain-based Access Control IoT systems ensure that the desired access controls are exercised and access to offered services is restricted only to those entities who are allowed to access it. Traditional Role Based Access Controls suffer from the problem of single point of control and failure. Blockchain based access control provides immutable, and smart contract based customizable access control mechanisms. Some prominent decentralized access control mechanisms are:

Attribute-Based Access Control (ABAC): This mechanism is more fine-grained and context-based. It either grants or revokes access depending on the Boolean rule set considering the attributes of the subject, object, and the environment (time and place, for example). The blockchain keeps track of the attributes and applies policies using smart contracts preventing any tampering with data.

Capability-Based Access Control (CapBAC): Here permissions are given in the form of capability tokens. To get access to a resource, one needs to show valid capability tokens, which can be withdrawn with the help of the blockchain.

Identity-Based Access Control (IBAC): The simplest of all methods when access control depends on an identity of a subject. It may involve using ACLs, which are stored on the blockchain.

4.4 Decentralized Access Control Models

The key consideration for distributed identity is ensuring privacy in addition to establishing identity. Through selective disclosure, it is possible to reveal claims in a VC selectively without having to disclose the complete dataset. For instance, it is possible to prove

an age greater than 18 years without disclosing one's actual date of birth.

Some of the approaches to enable this process include the following:

Zero-Knowledge Proof (ZKP): A ZKP technique enables the creation of proofs regarding certain claims made by a prover to a verifier without disclosing any underlying information. Modern zero-knowledge techniques such as zk-SNARKs [39] and zk-STARKs [40] are commonly used in eKYC processes to comply with regulations in complete data privacy. **Selective Disclosure Signatures:** Selective disclosure signatures employ cryptographic digital signatures to allow aggregation and removal claims. Table 5 provides Comparison of Identity Management Paradigms. Table 6 shows Decentralized Access Control Models in BCIoT.

5. SECURITY SERVICES AND DEFENSE SYSTEMS

The blockchain technology is the underlying technology behind cryptocurrency Bitcoin. As it was a cryptocurrency, by design blockchain has included essential security features in it. So, use of blockchain in IoT systems brings these security features of immutability, transparency, and availability. Thereby many security aspects irrespective of the underlying domain or application are implicitly covered.

5.1 Intrusion Detection Systems (IDS)

Blockchain based Intrusion Detection Systems can potentially revolutionize the attack surface by introducing immutable, traceable and tamper resistant immune systems to any deployed application. **Cooperative Blacklisting:** The distributed IDS system leverages the blockchain system to exchange characteristics of malicious packets and/or undesirable connection patterns within a network. By sharing information, the time-to-detection for any new attack is shortened.

Distributed Anomaly Detection: A lightweight framework such as CIoT [41] leverages blockchain technology to update the anomaly detection model using node attestation.

Domain-Specific Intrusion Detection System: In Internet of Vehicle (IoV), a micro blockchain system employs intrusion detection system to a location.

Table 5. Identity Management Paradigms

Feature	Centralized	Federated	SSI	Ref.
Control	Service Provider	Shared among organizations	User (Holder)	[11]
Data Storage	Central Database	Distributed Centralized	Personal Wallet / Edge	[5]
Trust Model	Single TTP	Mutual Trust	Decentralized (Blockchain)	[10]
User Privacy	Low	Medium	High (Selective Disclosure)	[10, 11]
Identifier	Username	SSO	DID / VC	[5, 10, 11]

There are applications of traceability using blockchain in several domains [42]. A collaborative intelligent system can be designed where multiple nodes in the network could contribute to threat detection rather than being dependent on a single centralized server.

Table 6. Decentralized Access Control Models

Model	Mechanism	Blockchain Role	Benefit	Ref.
RBAC	Role-based permissions	Auditing role assignments	Scalable for organizations	[13]
ABAC	Attribute-based policies	Policy storage and enforcement	Fine-grained control	[22]
ACL	Access permission lists	Immutable access logs	Simple implementation	[23]

Malicious network behavior could be identified by making use of blockchain and AES [43].

5.2 Blockchain Federated Learning (BlockFL)

Federated learning allows IoT devices to learn from their own accumulated data without sending it completely, sending only some trained parameters to the server. Unfortunately, classic federated learning suffers from two key issues: central server vulnerability to malfunctioning and susceptibility to poisoning attacks. To solve such problems, researchers introduced Blockchain Federated Learning (BlockFL), which uses a distributed ledger instead of a central server.

5.3 Mitigation of Distributed Denial-of-Service (DDoS)

IoT devices with default security provisions are vulnerable to botnets attacks, such as Mirai [44], which are used to choke servers with traffic and halt the services. Blockchain are immune to it by decentralizing networks.

Distributed Traffic Filtering: Blockchain-enabled gateways can delegate and collectively mark IP addresses as malicious. Once a DDoS attack is confirmed through a smart contract, the attack information is written to the ledger, directing all network entities to disconnect.

Resource Management: Frameworks like EdgeChain [45] utilize smart contracts to employ credit-linked resource management. If an edge node makes many quick requests, it is a sign of an attack, the system mitigates it.

6. TECHNICAL DIFFICULTIES AND RESEARCH CHALLENGES

Despite being a promising innovation for the future, BCIoT faces considerable technical barriers when it comes to deployment at large scale. Even though blockchain technology offers reliable security features, its incorporation in IoT comes with inherent trade-offs due to its resource-consuming processes against the constrained features of IoT devices. In this section, the main barriers to BCIoT will be explored.

6.1 Scalability and Performance Bottlenecks

In case of IoT devices the amount of data generated is humongous, as the amount of data to be processed increases the system should also scale up to handle large volumes of data. Scalability is the ability of the system under operation to increase its capacity to manage higher load by increasing its resources in such a way that the thresholds of the parameters like throughput and latency are in acceptable

Table 7. Blockchain-Enhanced Security Services

Service	Blockchain Role	Benefit	Models	Ref.
IDS	Distributed threat-signature storage	Collaborative threat intelligence; no SPOF	CIoTA, BFF-IDS	[41,43]
BlockFL	Decentralized model aggregation and verification	Resistant to poisoning attacks; privacy-preserving ML	BlockFedML	[22,46]
Anti-DDoS	Smart-contract-based collaborative blacklisting	Botnet mitigation at gateway level	Co-IoT, EdgeChain	[44,47]

range.

Transaction Throughput and Latency: Existing public blockchains feature extremely low throughput measured in transactions per second (about 5 for Bitcoin and 15 for Ethereum), which is much lower than that of VISA (up to 8500 TPS) [13]. High latency involved in transaction confirmations (seconds/minutes) makes the technology not suitable for time-sensitive operations, such as autonomous vehicles coordination or production line automation.

The Endless Ledger: Blockchain technology requires storing all transaction information on each node. Now, the size of the Bitcoin ledger exceeded 740 GB; Ethereum's is growing rapidly. Storing this amount of data on IoT nodes becomes an issue.

Network Bandwidth and Propagation: Broadcasting transactions over a Peer-to-Peer network can create a lot of communication overhead. Massive deployment could create "broadcast storms" where the number of synchronization messages will consume all the bandwidth available in the network.

6.2 Resource Constraints in IoT Environments

IoT entities have less resources, memory capacity, and bandwidth. These limitations contradict with what is expected of blockchain systems:

Resource Intensive Algorithms: The consensus algorithms, like Proof-of-Work (PoW), are by design should use lots of computational resources to ensure security. Further running smart contracts on these low-end devices may be very difficult.

Rapid Battery Drain: Heavy use of cryptography (digital signatures and message verifications), combined with constant listening to the network for synchronizations, drains the batteries fast. It has become a major issue for faraway sensors and IoT health monitoring devices.

Limited Data Storage: Generally, sensors simply do not have sufficient memory or storage capacity to temporarily save their own data as transactions.

7. FUTURE WORK OPTIONS

Though Blockchain with IoT can address various shortcomings of the traditional systems, as developments are going on in quantum computing, more resilient approaches should be considered. This section discusses future work options in this area of BCIoT through post Quantum security and Zero Trust Architectures.

7.1 Post-Quantum Blockchain Security for IoT

The conventional blockchain architecture depends largely on asymmetric cryptosystems such as RSA and ECC which are not protected by future quantum-based systems. Shor's algorithm [48], for example, will be able to break present digital signatures, whereas Grover's algorithm [49] would limit the usefulness of hash approaches (e.g., SHA-256) and cause 51% attacks.

Post-Quantum Cryptography (PQC) Algorithms Standardization: Research in this area should focus on combining NIST-approved post-quantum cryptographic algorithms with BCIoT.

Overcoming the Size Barrier: One of the challenges of implementing PQC algorithms is their need for much larger keys and signatures compared to classical schemes. This problem should be addressed by either creating lightweight post-quantum algorithms or employing hardware solutions in the form of TEEs.

Hybrid PKI Frameworks: To address the issue of transitioning from existing systems to future ones, scientists are investigating the use of hybrid models of public-key infrastructure that will include both classical and post-quantum signatures.

7.2 Transitioning to Zero Trust Architecture (ZTA)

Zero Trust Architectures [8] by default considers every entity in the system as untrusted, and it works on the principle of "Never trust, Always Verify". All the access requests are dynamically validated. Continuous and Context-Aware Authentication: Instead of a one-off authentication process, ZTA involves ongoing authentication that considers the behavior of the device, its location, and other environmental factors. This behavior could be recorded in a distributed ledger provided by blockchain technology.

Micro-Segmentation and Software Defined Perimeter (SDP): SDPs have the potential of creating overlays of network security through which resources will not be accessible to unauthorized users. The challenge is how to implement blockchain-based access control in conjunction with Network Function Virtualization.

Risk-Aware Access Control: As the concept of Role-Based Access Control (RBAC) evolves, ZTA requires that IoT access is granted based on the level of risk posed by each access attempt.

7.3 Future Prospects of Blockchain with IoT

Future works should cover lightweight post-quantum cryptographic primitives to defend resource-aware IoT systems with emerging quantum threats [7] in consideration. Integrating Zero Trust verification and blockchain interoperability will create dependable trust across large-scale implementations. [8, 13].

8. CONCLUSION

Protecting IoT devices is a key component in any smart city or critical infrastructure, and securing these devices, as well as the data they transmit, is crucial. BCIoT tackles structural weaknesses of centralized systems by deploying consensus-based solutions, tamper-proof ledgers and cryptographic auditability across IoMT, IoV, and smart municipal grids. Moreover, the addition of Self-Sovereign Identity (SSI) and Decentralized Identifiers (DID) puts identity governance in the hands of the users, and Blockchain Federated Learning (BlockFL) and collaborative intrusion detection systems add another layer of protection against adversarial manipulation.

However, in order to achieve scalable real-world deployment, it is necessary to address issues of high transaction latency, network bloat, and device limitations through lightweight consensus and

Table 8. PQC Types for IoT

Category	Problem	Pros	Cons	Algorithms	Ref.
Lattice-Based	SVP	Fast, balanced performance	Complex implementation	Kyber, Dilithium, FALCON	[50, 51]
Hash-Based	One-way functions	High security, small keys	Large signatures	SPHINCS+, XMSS	[52, 53]
Code-Based	Error-correction codes	Fast verification	Large public keys	Classic McEliece	[54]
Isogeny-Based	Supersingular isogenies	Small key/signature sizes	High computational latency	SIKE (deprecated)	[55]

off-chain storage structures. At the same time, the long-term resistance to new ways of computing requires the proactive implementation of Post-Quantum Cryptography (PQC), and Zero Trust Architectures (ZTA), thereby laying a solid groundwork for future decentralized cyber-physical systems.

9. REFERENCES

- [1] L. D. Xu, Y. Lu, and L. Li. Embedding blockchain technology into IoT for security: A survey. *IEEE Internet of Things Journal*, 8(13):10452–10473, 2021.
- [2] A. A. Jolfaei, S. F. Aghili, and D. Singelee. A survey on blockchain-based IoMT systems: Towards scalability. *IEEE Access*, 9:148948–148975, 2021.
- [3] A. H. Allam, I. Gomaa, H. H. Zayed, and M. Taha. IoT-based eHealth using blockchain technology: A survey. *Cluster Computing*, 27(6):7083–7110, 2024.
- [4] L. Zheng, T. Feng, Z. Xie, X. Li, and C. Su. BARM: Blockchain-assisted anonymous authentication and reputation management for mobile crowdsensing in Internet of Vehicles. *IEEE Internet of Things Journal*, 2025. early access.
- [5] A. El-Fatyany, J. Mahmood, M. A. Berwo, X. Wang, L. Lu, Q. Xue, and K. Ren. Intrusion detection and prevention for intra- and inter-vehicle networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 2026. early access.
- [6] R. Alkadi, N. Alnuaimi, C. Y. Yeun, and A. Shoufan. Blockchain interoperability in unmanned aerial vehicles networks: State-of-the-art and open issues. *IEEE Access*, 10:14463–14479, 2022.
- [7] H. Gharavi, J. Granjal, and E. Monteiro. Post-quantum blockchain security for the Internet of Things: Survey and research directions. *IEEE Communications Surveys & Tutorials*, 26(3):1748–1774, 2024.
- [8] N. F. Syed, S. W. Shah, A. Shaghghi, A. Anwar, Z. Baig, and R. Doss. Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access*, 10:57143–57179, 2022.
- [9] I. Ahmed, K. Toyoda, T. Nakano, S. Kasahara, S. R. Goyal, and T. H. Tran. A systematic review on blockchain-enabled eKYC: Leveraging SSI and DID for secure and efficient identity verification. *IEEE Internet of Things Journal*, 2025. early access.

- [10] A. S. Al-Mulla and M. H. Ali. Privacy-aware blockchain-based access control architecture for securing edge-computed Internet of Things node data pipelines. *ITEGAM-Journal of Engineering and Technology for Industrial Applications*, 12(58):45–54, 2026.
- [11] O. A. Bello and K. M. Yusuf. Risk management and governance frameworks in blockchain-based decentralized identity projects. *ITEGAM-Journal of Engineering and Technology for Industrial Applications*, 11(54):172–180, 2025.
- [12] X. Zhou et al. Decentralized federated graph learning with lightweight zero trust architecture for next-generation networking security. *IEEE Journal on Selected Areas in Communications*, 43(6):1908–1922, June 2025.
- [13] T. A. Alghamdi, R. Khalid, and N. Javaid. A survey of blockchain-based systems: Scalability issues and solutions, applications and future challenges. *IEEE Access*, 12:79626–79651, 2024.
- [14] S. K. Nair, V. Sharma, and P. K. Gupta. BlockArc: A blockchain based smart contract for reward verification in automated edge environments. *ITEGAM-Journal of Engineering and Technology for Industrial Applications*, 11(54):181–192, 2025.
- [15] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, Bitcoin.org, 2008.
- [16] Vitalik Buterin. Ethereum white paper. *GitHub Repository*, 1:5–7, 2013.
- [17] Gavin Wood. Polkadot: Vision for a heterogeneous multi-chain framework. *White Paper*, 21:4662, 2016.
- [18] Christian Cachin. Architecture of the Hyperledger blockchain fabric. In *Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers*, pages 1–4, 2016.
- [19] J. Liu. Blockchain meets AI in healthcare: A review of convergent technologies for digital health transformation. *Frontiers in Blockchain*, 9, 2026.
- [20] I. Butun and P. Osterberg. A review of distributed access control for blockchain systems towards securing the Internet of Things. *IEEE Access*, 9:5428–5441, 2021.
- [21] E. A. Shammam, A. T. Zahary, and A. A. Al-Shargabi. A survey of IoT and blockchain integration: Security perspective. *IEEE Access*, 9:156114–156150, 2021.
- [22] Y. Jiang, B. Ma, X. Wang, G. Yu, P. Yu, Z. Wang, W. Ni, and R. P. Liu. Blockchain federated learning for Internet of Things: A comprehensive survey. *ACM Computing Surveys*, 56(10):1–37, 2024.
- [23] J.P. Morgan. Quorum whitepaper v0.2. Technical report, ConsenSys Quorum Repository, 2016.
- [24] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun. On the security and performance of proof of work blockchains. In *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, pages 3–16, 2016.
- [25] F. Saleh. Blockchain without waste: Proof-of-stake. *Review of Financial Studies*, 34(3):1156–1190, 2021.
- [26] M. Castro and B. Liskov. Practical Byzantine fault tolerance. In *Proc. 3rd Symp. Operating Syst. Design Implement. (OSDI)*, pages 173–186, 1999.
- [27] D. Larimer. Delegated proof of stake consensus. White paper, BitShares, 2014.
- [28] Hyperledger Labs. Proof of elapsed time 2 (PoET2) lab specification. Technical report, Linux Foundation Decentralized Trust Labs, 2020.
- [29] A. Ekblaw et al. MedRec: Blockchain for medical data access, permission management and trend analysis. MIT Media Lab, 2016.
- [30] HealthChain. HealthChain official website. <https://healthchain.com/>, 2026. Accessed: May 2026.
- [31] J. Zhang, Y. Jiang, J. Cui, D. He, I. Bolodurina, and H. Zhong. DBCPA: Dual blockchain-assisted conditional privacy-preserving authentication framework and protocol for vehicular ad hoc networks. *IEEE Transactions on Mobile Computing*, 23(2):1127–1141, 2022.
- [32] A. Vangala, B. Bera, S. Saha, A. K. Das, N. Kumar, and Y. Park. Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems. *IEEE Sensors Journal*, 21(14):15824–15838, 2021.
- [33] A. Jain, S. Barke, M. Garg, A. Gupta, B. Narwal, A. K. Mohapatra, D. K. Sharma, and G. Srivastava. A walkthrough of blockchain-based Internet of Drones architectures. *IEEE Internet of Things Journal*, 11(21):34924–34940, 2024.
- [34] A. Padma and M. Ramaiah. Blockchain-based an efficient and secure privacy-preserved framework for smart cities. *IEEE Access*, 12:21985–22002, 2024.
- [35] Ryoshi. The Shiba Inu WoofPaper: An experiment in decentralized spontaneous community building. White paper, v2, Shiba Inu, 2021.
- [36] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers & Security*, 88:101653, 2020.
- [37] Datapace Team. Datapace: Decentralized data marketplace based on blockchain and global network of sensors. White paper, Nokia Open Ecosystem Network, 2019.
- [38] N. Mansoor, K. F. Antora, P. Deb, T. A. Arman, A. A. Manaf, and M. Zareei. A review of blockchain approaches for KYC. *IEEE Access*, 11:121013–121042, 2023.
- [39] N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer. From garbled circuits to efficient zero-knowledge arguments for NP. In *Proc. 32nd Annu. Cryptol. Conf. (CRYPTO)*, pages 326–345, 2012.
- [40] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev. Scalable, transparent, and post-quantum secure computational integrity. *IACR Cryptology ePrint Archive*, 2018:46, 2018.
- [41] T. Golomb, Y. Mirsky, and Y. Elovici. CIoT: Collaborative IoT anomaly detection via blockchain. In *Proc. NDSS Workshop Decentralized IoT Secur. Privacy (DISP)*, 2018.
- [42] T. T. Baladraf and M. Marimin. Potential adoption of blockchain in food cold supply chain: A bibliometric study and future research agenda. *ITEGAM-Journal of Engineering and Technology for Industrial Applications*, 11(52):112–125, 2025.
- [43] H. Uppala and R. R. Devi. AES-enhanced blockchain intrusion detection system for secure networks. *ITEGAM-Journal of Engineering and Technology for Industrial Applications*, 12(58):12–21, 2026.
- [44] M. Antonakakis et al. Understanding the Mirai botnet. In *Proc. 26th USENIX Security Symposium*, pages 1093–1110, 2017.
- [45] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, and Y. Zhao. EdgeChain: An edge-IoT framework and prototype based on

blockchain and smart contracts. *IEEE Internet of Things Journal*, 6(3):4719–4732, 2019.

- [46] J. Wang, J. Wang, Q. Zhang, and H. Wang. BlockFedML: Blockchain federated machine learning systems. In *Proc. Cyber-Enabled Distrib. Comput. Knowl. Discov. (CyberC)*, pages 162–169, 2019.
- [47] Z. Abou El Houda, A. S. Hafid, and L. Khoukhi. Co-IoT: A collaborative DDoS mitigation scheme in IoT environment based on blockchain using SDN. In *Proc. IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, 2019.
- [48] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proc. 35th Annu. Symp. Found. Comput. Sci. (FOCS)*, pages 124–134, 1994.
- [49] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. 28th Annu. ACM Symp. Theory Comput. (STOC)*, pages 212–219, 1996.
- [50] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé. CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. In *Proc. IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 353–367, 2018.
- [51] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé. CRYSTALS-Dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018(1):238–268, 2018.
- [52] D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, and P. Schwabe. The SPHINCS+ signature framework. In *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, pages 2129–2146, 2019.
- [53] A. Hülsing. WOTS+ — shorter signatures for XMSS and SPHINCS. In *Proc. Int. Conf. Post-Quantum Cryptogr. (PQCrypto)*, pages 141–155, 2013.
- [54] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. Technical Report DSN Progress Report 42-44, Jet Propulsion Laboratory, California Institute of Technology, 1978.
- [55] D. Jao and L. De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *Proc. 4th Int. Workshop Post-Quantum Cryptogr. (PQCrypto)*, pages 19–34, 2011.