RESEARCH-ARTICLE

Blockchain-Enabled SDN Audit System for On-chain Off-chain Communication Networks

DAMING HUANG, Nanjing University, Nanjing, Jiangsu, China

JINCHENG XIANG, Nanjing University, Nanjing, Jiangsu, China

YU JIN, Nanjing University, Nanjing, Jiangsu, China

CHEN TIAN, Nanjing University, Nanjing, Jiangsu, China

Open Access Support provided by:

Nanjing University

Published: 01 December 2025

Citation in BibTeX format

CoNEXT '25:The 21st International Conference on emerging Networking EXperiments and Technologies
December 1 - 4, 2025
Hong Kong, Hong Kong

Conference Sponsors:
SIGCOMM

BlockNetSys '25: Proceedings of the 2025 ACM CoNEXT Workshop on Blockchain-Network Synergy (December 2025)
https://doi.org/10.1145/3769698.3771230
ISBN: 9798400722448

Blockchain-Enabled SDN Audit System for On-chain Off-chain Communication Networks

Daming Huang
State Key Laboratory for Novel Software Technology
Nanjing University
Nanjing, Jiangsu, china
huangdm@nju.edu.cn

Jincheng Xiang
State Key Laboratory for Novel Software Technology
Nanjing University
Nanjing, Jiangsu, china
jinchengxiang@smail.nju.edu.cn

Yu Jin
State Key Laboratory for Novel Software Technology
Nanjing University
Nanjing, Jiangsu, china
jiny2048@gmail.com

Chen Tian
State Key Laboratory for Novel Software Technology
Nanjing University
Nanjing, Jiangsu, china
tianchen@nju.edu.cn

Abstract

This paper proposes a blockchain-based SDN auditing system, suitable for auditing communication events occurring in off-chain networks between smart edge gateways and terminals within the context of trustworthy on-chain off-chain SDN management communication networks, thereby meeting the requirements for full communication supervision. The method not only audits all SDN communication management events in the off-chain SDN network related to on-chain off-chain trustworthy interactions, but also securely stores the audit data through a combination of the security supervision chain and IPFS, ensuring the trustworthy and reliable storage of audit data while achieving efficient data storage.

CCS Concepts

• **Networks** → **Network monitoring**; • **Information systems** → **Data management systems**; • **Security and privacy** → Domain-specific security and privacy architectures.

Keywords

Audit System; SDN; Blockchain; On-chain Off-chain Communication

ACM Reference Format:
Daming Huang, Jincheng Xiang, Yu Jin, and Chen Tian. 2025. Blockchain-Enabled SDN Audit System for On-chain Off-chain Communication Networks. In *Proceedings of the 2025 ACM CoNEXT Workshop on Blockchain-Network Synergy (BlockNetSys '25), December 1–4, 2025, Hong Kong, Hong Kong*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3769698.3771230

BlockNetSys '25, Hong Kong, Hong Kong

ACM ISBN 979-8-4007-2244-8/2025/12
https://doi.org/10.1145/3769698.3771230

1 Introduction

During the evolution of blockchain technology from the 1.0 to the 3.0 era, a distinct trend has emerged: the application ecosystem is gradually shifting from one based solely on chain-native functionalities towards one characterized by on-chain and off-chain collaboration. By integrating the advantages of established off-chain technologies with the trustworthy collaboration capabilities inherent to on-chain systems, blockchain technology can better serve practical requirements, allowing blockchain systems to demonstrate enhanced strengths. This necessitates leveraging the core technical advantages of blockchain—namely tamper resistance and traceability of on-chain data—while simultaneously circumventing its limitations, such as high consensus overhead and constrained performance. Consequently, it is essential to design a software-defined trusted and secure interaction framework that balances generality and flexibility.

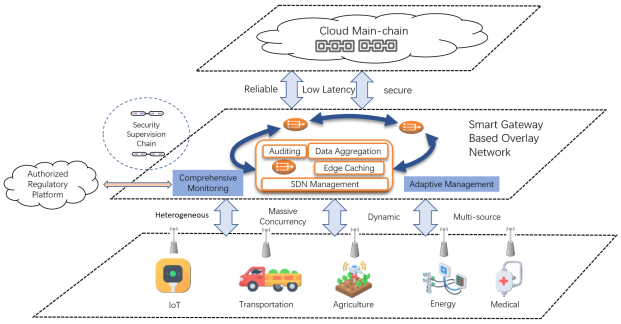

Figure 1: end-edge-chain communication architecture

A critical issue in the research on trusted on-chain/off-chain interaction is the design and implementation of low-latency, high-security, adaptive, and regulatable network-communication techniques that bridge on-chain and off-chain environments. As illustrated in Figure 1, data originating from distinct administrative domains—including agriculture, healthcare, energy, transportation, and industrial Internet—must be committed to cloud-based blockchains. To ensure efficient, reliable, and secure data transmission, we propose a three-tier End-Edge-Chain communication

architecture composed of end devices, smart edge gateways, and the cloud blockchain.

Within such an on-chain/off-chain communication network architecture, to meet regulatory compliance requirements, it is necessary to conduct comprehensive auditing of all communication events during on-chain/off-chain interactions and fulfill the supervision demands of authoritative entities. Since all terminal data from application management domains must traverse smart edge gateways for on-chain processing, embedding an auditing component within these gateways enables comprehensive auditing of all communication events directed towards the blockchain. However, communication between terminals and smart edge gateways may remain dynamic and heterogeneous. Crucially, as communication between off-chain terminals and smart edge gateways is managed by a distributed Software-Defined Networking (SDN) system, implementing comprehensive auditing within the SDN system serves as a vital complementary measure to the auditing performed at the smart edge gateways.

The essence of auditing is to address information asymmetry and the lack of trust. By applying blockchain technology to the automated auditing of information systems, issues such as information asymmetry, data tampering, data distortion, the need for trusted third parties, and single points of failure can be inherently resolved. This is not merely an upgrade of auditing tools, but a fundamental reshaping of the auditing paradigm. [22] [17].

The remainder of this paper is organized as follows. Section 2 reviews the state of the art in blockchain-empowered auditing and SDN-oriented auditing. Section 3 elaborates on the design of the on-chain/off-chain communication network and precisely identifies the communication behaviors that must be audited. Section 4 presents the design of our blockchain-empowered distributed SDN auditing system. Section 5 details our implementation and experimental evaluation, while Section 6 concludes the paper.

2 Related Work

From the perspective of blockchain addressing the credibility and tamper-resistance of traditional audit logs, several representative works exist. BlockAudit [2] extends ORM layer to enable seamless transformation of traditional audit logs into blockchain transactions. This is achieved by leveraging Hyperledger Fabric to create a decentralized log storage system. The network achieves low latency within 30 nodes while maintaining security and audit integrity. Audita [7] is a chain-level storage audit framework that balances scalability, decentralization, and data integrity. It innovatively integrates PDP (Proof of Delivery) verification mechanisms with the blockchain out-block process.

Blockchain's application to cloud auditing is a vital research area. ProvChain [11] integrates blockchain with cloud data provenance, ensuring tamper-resistance, privacy, availability, and low overhead. Mishra et al. [14] propose a decentralized framework combining redactable blockchain and encrypted deduplication to ensure integrity, reduce redundancy, preserve privacy, and remove third-party auditors. Wang et al. [18] design a TPA-free scheme using blockchain, edge computing, and homomorphic hashing for cost-efficient integrity verification, but neglect edge node trust and storage bloat. Hossain et al. [10] survey blockchain auditing and propose a framework with multi-cloud storage and privacy techniques to ensure integrity, privacy, and audit trust. Dwivedi et al. [6] delegate verification to edge servers and log only failures on-chain for real-time tamper detection with low owner overhead. BOCS [19] implements lightweight vehicular cloud auditing via non-interactive evidence and smart contracts.

Blockchain research increasingly addresses auditing challenges across sectors. BlockTrail [3] employs a layered multi-chain design with optimized PBFT, achieving high-throughput, low-storage auditing for government use. Adlam et al. [1] present a permissioned Hyperledger Fabric-based audit log for EHRs, featuring a decentralized, immutable COt mechanism. López-Pimentel et al. [12] propose a hybrid architecture hashing microservices data while ensuring audit traceability and completeness. Dong et al. [5] apply Hyperledger Fabric to audit IoT data completeness, solving TPA centralization with an anonymous, fair, and accountable system.

Notable efforts also explore hybrid on-chain/off-chain auditing approaches. Malhotra et al. [13] pioneers a chain-based audit method that combines IPFS storage for source material, XAI explanation, and SHA256 hashing with timestamps to provide a secure and tamper-resistant AI decision-making process.

Auditing related to blockchain enabled application security represents another active area of investigation. SILedger [15] implements a blockchain and ABET-based access control system for cross-domain SIApps, resolving SDN-IoT permission fragmentation and unreliability. Cumulus [4] is a blockchain data audit protocol using state channels to ensure privacy, fairness, and integrity in collaborations. Zhao et al.[21] integrate end-to-end blockchain governance with deep belief networks for trustworthy audit-trail reconstruction and anomaly detection.

Significant progress has been made in SDN network auditing. Yu et al. [20] developed a "Virtual Routing" audit mechanism in SDN controllers, simulating third-party flow table modifications to detect routing loops. Herbaut et al. [9] introduced an intent-based layer for auditing SDN security policy consistency, improving scalability across large networks. NFAudit [16] is a flexible, low-overhead framework using probabilistic sampling and trusted execution to verify third-party network function trustworthiness. Guan et al. [8] proposed a blockchain-based SDN auditing scheme with distributed key-generation. By deploying switch-level agents in a consortium chain, it enables trustable cross-domain auditing for decentralized SDNs.

The distinction of this work from the aforementioned studies lies in its integration of blockchain technology with SDN technology within the framework of trusted on-chain/off-chain interaction. This approach enables comprehensive auditing of all SDN management-related communication events within the cross-domain off-chain network spanning between terminals and smart edge gateways. Crucially, the auditing scope encompasses not only communication events between terminals and smart edge gateways but also self-auditing within the distributed SDN system itself. Furthermore, this work contributes research on the differentiated storage (on-chain vs. off-chain) and optimized storage of audit data.

3 Definition of On-chain Off-chain SDN Network Commnunication Events

3.1 Overview of On-Chain and Off-Chain Communication Networks

As illustrated in Figure 1, application terminals residing in distinct administrative domains upload their data through intelligent edge gateways, which subsequently anchor the transactions into the cloud-end blockchain. Under nominal conditions, each terminal performs mutual authentication with its domain-specific gateway, and the resulting payload is committed via that gateway. To tolerate volatile off-chain topologies and gateway failures, a security supervision chain orchestrates a distributed SDN fabric that continuously adapts the underlying communication paths.

The authentication credentials for smart edge gateways, end devices, and the SDN controller comprise a triple (Identity ID, Public Key, Private Key). During identity registration, each entity's Identity ID and Public Key are stored on the security supervision chain. The Private Key, however, is retained solely by the respective communicating entity itself. This architecture establishes a decentralized authentication framework.

Within each administrative domain, the local SDN controller governs the off-chain substrate comprising the domain's intelligent edge gateway and its collocated front-end SDN switch; every packet destined for the gateway is obliged to traverse this switch. Both gateways and controllers periodically publish their liveness and telemetry records to the security supervision chain. By aggregating these submissions, the security supervision chain materializes a unified view of the global network and of the distributed SDN control plane, yielding a fully decentralized SDN architecture.

Upon detecting a failure in a smart edge gateway, the responsible SDN controller identifies the gateway's faulty status and selects an optimally underutilized operational gateway as a candidate based on the global network state. Concurrently, the controller installs flow rules on the upstream SDN switch of the failed gateway, redirecting terminal traffic originally destined for the failed gateway to itself. The controller then extracts terminal information from received PACKET-IN messages, negotiates with the affected terminals, and reconfigures their on-chain data paths to utilize the selected low-load candidate gateway. This process achieves restoration of the on-chain data transmission paths.

Upon detecting the failure of an SDN controller, the security supervision chain inspects the global SDN state to elect the controller exhibiting the lightest instantaneous load as the guardian node. This guardian then imports the security supervision chain's decision record and seamlessly assumes the management responsibilities of the failed controller, thereby restoring fault tolerance to the distributed SDN control plane without centralized intervention.

Consequently, to enable end-to-end auditing of the off-chain SDN fabric, the events that must be persisted are derived from (i) the control-plane decisions issued by SDN controllers and (ii) the data-plane interactions among communicating entities, as catalogued in Table 1.

3.2 SDN Controller-Generated Communication Events

SDN controller-generated communication events primarily occur in the following three scenarios. Refer to Table 1 for specific data fields of each event: (1) When an SDN controller detects a failure in a smart edge gateway within its managed domain, after calculating the least-loaded candidate gateway, it must install flow rules on the upstream SDN switch of the failed smart edge gateway. This constitutes a critical step for recovery data on-chain path operations, thus requiring generation of relevant audit events. Two correlated events are produced: One being the flow rule deployed to the switch. The other being load metrics of currently operational smart edge gateways. (2) Upon installing upstream-traffic redirection flow entries on the SDN switch that immediately precedes a faulty gateway, all packets destined for that gateway are redirected to the supervisory SDN controller and manifest as PACKET-IN messages. (3) The security supervision chain assigns a guardian SDN controller to each operational controller based on a synthesized, global SDN view, and synchronizes this assignment across all controllers. When any SDN controller fails, its guardian detects the failure instantly and assumes responsibility for the failed controller's management domain. The guardian then emits a takeover communication event.

3.3 Entity-Interaction Communication Event

In off-chain edge networks, there are three principal communication entities: smart edge gateways, SDN controllers, and end devices. Prior to any exchange, these entities must mutually authenticate and subsequently rely on secure communication protocols to preserve the integrity of off-chain communications. When an end device submits data to a gateway, mutual authentication between the device and the smart edge gateway is mandatory. All authentication steps and subsequent communication actions involving the gateway are logged by an auditing component embedded within the smart edge gateway itself. Smart edge gateways and SDN controllers do not communicate directly; instead, SDN controllers manage and safeguard gateways via the security supervision chain. Upon gateway failure, the SDN controller repairs the data-on-chain path by negotiating candidate gateways with the end devices. Consequently, the distributed SDN system must provide comprehensive auditability of all interactions between SDN controllers and end devices.

Within the SDN controller, terminal authentication records — including terminal ID, authentication result, and timestamp—are logged. This information is stored both in local storage and the security supervision chain, with synchronous replication to the regulatory network. Considering terminal performance and energy constraints, only authentication failures (involving SDN controllers and gateways) need be recorded to the security supervision chain. These records can be asynchronously synchronized to the regulatory network by a regulatory daemon during periodic maintenance. Refer to Table 1 for detailed audit event specifications

Table 1: Communication Audit Event

Category	Communication Audit Event	Audit Field
SDN Data Transmission Path Recovery	Flow Table	SDN Controller ID, Switch ID, Timestamp, Match (OFPMatch object denoting matching rule), Instructions (ordered list of execution directives), Priority (flow-entry precedence level), Cookie (controller-assigned flow identifier), Command (type of flow-table operation), Flags (bitmask governing flow-entry behavior)
SDN Data Transmission Path Recovery	Operational Gateway Load Metric	SDN Controller ID, Timestamp, Operational Intelligent Edge Gateway Load Metric List (Gateway1ID, Gateway1LoadMetric),..., (GatewaynID, GatewaynLoadMetric)
SDN Data Transmission Path Recovery	Packet-in Message	SDN Controller ID, Ingress Switch Datapath ID, Timestamp, OpenFlow Version, Ingress Port, Source/Destination MAC Address, EtherType, Source/Destination IPv4 Address, IP Protocol Number, TCP/UDP Source/Destination Port, Complete Raw Packet Byte Stream, Total Packet Length (Bytes), Packet-In Trigger Reason, Matched Flow Entry ID
Distributed SDN System	Guard SDN Controller Takeover	Failed SDN Controller ID, Guard SDN Controller ID, Timestamp
Communication Entity Interaction	SDN Controller-to-End-Device Authentication	SDN Controller ID, End-Device ID, Authentication Result, Timestamp
Communication Entity Interaction	End-Device-to-SDN Controller Failed Authentication	SDN Controller ID, End-Device ID, Timestamp

4 Blockchain-Enabled SDN Audit

4.1 Audit System Desgin

The architecture of the blockchain-based distributed SDN auditing system is depicted in Figure 2. Within each SDN controller, whenever a communication event under SDN governance occurs, the SDN Network Management Module dispatches the event to the SDN Auditing Module. The SDN Auditing Module subsequently derives a high-level semantic representation and a cryptographic hash of the communication event. The SDN Communication Event Aggregation Module then attempts to coalesce semantically identical events, thereby minimizing storage and processing overhead. Finally, the SDN Auditing Module persists the full communication audit events to the IPFS network, while recording both the high-level semantic representation and the hash of each event on the security supervision chain. Concurrently, these condensed audit artifacts are forwarded to the centralized platform of the authoritative regulatory body via a dedicated auditing network.

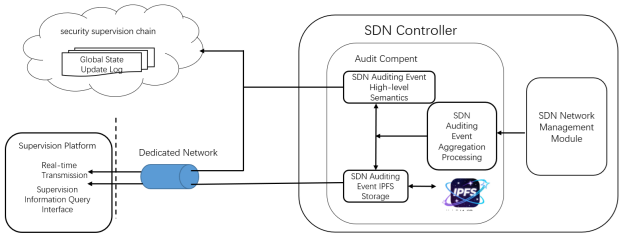

Figure 2: Blockchain-Enabled SDN Audit System Desgin

4.2 On-chain/Off-chain Hybrid Trusted Audit-Data Storage

Persisting every auditable event of the on-chain/off-chain SDN auditing system to the security-monitoring sidechain guarantees tamper-evident storage, yet during traffic spikes the audit volume becomes prohibitive. This forces the auditing layer to expend excessive resources on bulk on-chain ingestion and saturates the security supervision chain with consensus and storage overhead. Consequently, audit-data persistence must follow the "fat-off-chain, thin-on-chain" paradigm.

We therefore adopt a tiered strategy for SDN audit data. Events that are low-volume yet critical to oversight and security—e.g., flow-table snapshots, operational gateway load metrics, guardian-controller takeover events, SDN-controller-to-end-device authentication, and end-device authentication failures—are persisted in full on the security supervision chain. In contrast, high-volume PACKET-IN events are handled differently: the raw packets are stored off-chain in IPFS, while their higher-level semantic summaries, cryptographic hashes, and IPFS addresses are committed on-chain. IPFS is chosen because local per-controller storage risks single-point failures and data loss; IPFS mitigates this risk. Owing to IPFS performance limitations, migration to a distributed database remains a future direction.

4.3 Audit-Data Reduction

The volume of PACKET-IN messages can be enormous; we therefore adopt an audit-data reduction policy. First, only those PACKET-IN messages generated by data-onboarding path repair are retained—any others are discarded. Second, because multiple PACKET-INs from the same end device may arrive within a short interval, we aggregate at a one-second granularity, preserving only a single representative PACKET-IN per device, as their functional effect is identical.

4.4 Audit-Data Delayed On-Chain Strategy

During peak audit data generation periods, immediate on-chain storage of all audit records may prove infeasible due to inherent blockchain throughput limitations. To address this, we implement a delayed commitment strategy:

- At peak load, only cryptographic hashes of audit data are committed to the chain
- Raw audit data is temporarily persisted in off-chain IPFS storage
- During off-peak periods, buffered audit data is asynchronously uploaded to the chain
- Automated hash verification ensures data integrity throughout this staged process

The audit module assesses system load by measuring the time required to process newly generated audit data. If the time taken to process a batch of freshly generated data exceeds a predefined threshold (e.g., 2 seconds), it is determined that either the volume of new data is substantial or the workload of the security supervision chain is high. Should processing time exceed 2 seconds for three consecutive processing cycles, the system is deemed to be in a high-load phase, triggering the automatic activation of the delayed on-chain mode for audit data.

When no newly generated audit data is detected or the processing time for a single batch of fresh data falls below a predefined threshold (e.g., 0.2 seconds), the audit system determines that the system is in a light-load phase. Then the audit system executes the following procedure:

- Retrieves delayed on-chain information from the blockchain.
- Fetches temporarily stored audit logs from IPFS using the retrieved Content Identifier (CID).
- Validates data integrity by comparing hash values read from the chain with those computed from the local logs.
- Upon successful integrity verification, parses the temporarily stored audit logs.
- Executes the on-chain process for each log entry sequentially.

4.5 SDN Management Behavior Compliance Verification

One design objective of the hybrid on-chain/off-chain communication network is to aggregate communication resources across management domains, enabling efficient, reliable, and adaptive on-chain data delivery by end devices. For security reasons, however, domain-specific policies may be enforced—e.g., when a failed gateway resides in a high-security domain, candidate gateways must be selected from domains of equal or higher classification, and data must never be redirected to gateways in lower-classification domains. To guarantee that SDN controllers respect these policies during path-repair operations, security rules can be pre-configured on the security supervision chain and subsequently downloaded to each controller. When SDN management events are committed on-chain, compliance smart contracts on the security supervision chain audit these events in real time, immediately detecting any non-compliant SDN management actions.

5 Implementation and Evaluation

To validate the feasibility of the Audit system, we set up a testbed using four servers, with each server simulating a smart edge gateway. Each server is also equipped with an OVS switch to simulate the front-end SDN switch of the gateway. The security supervision chain utilizes FISCO BCOS.

Table 2: Audit Log Processing Throughput Comparison

magnitudes of PACKET-IN messages	normal audit data saving mode throughput(log/s)	delayed on-chain strategy mode throughput(log/s)
2500	31.4	54.1
4000	27.2	51.9
6000	22.9	49.8

The hardware configuration of each gateway is an Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz with 257,616MB of memory. The software environment consists of the Ubuntu 22 operating system, Ryu controller, Python 3.8.10. Each gateway deploys our custom-developed terminal data on-chain service.

From the perspective of functional evaluation, we simulated scenarios on the testbed where failures of the smart edge gateway and SDN controller might occur during the process of terminal data transmission to the cloud blockchain. All relevant audit events were successfully recorded on the security supervision chain and the local IPFS network, confirming the effectiveness and correctness of our approach.

From the perspective of performance evaluation, we used Mininet to simulate 50 terminals submitting data for on-chain storage to the same server. We measured the log processing throughput rate of the SDN controller when saving audit data during path switching events. This measurement encompassed the time taken to save logs to the IPFS network and subsequently commit them to the security supervision chain. We tested the difference in log processing throughput rate between the normal audit data saving mode and the delayed on-chain strategy mode when handling different magnitudes of PACKET-IN messages, as detailed in Table 2. The experimental results demonstrate that the efficiency is significantly enhanced when employing the delayed on-chain strategy.

6 Conclusion

In response to the communication network security and full audit requirements for trustworthy on-chain off-chain interaction systems, this paper presents a blockchain-enabled SDN network auditing system. By integrating auditing components in the SDN controller with smart edge gateways and terminals, the system is capable of auditing network events occurring in the off-chain network between smart edge gateways and terminals, providing a valuable complement to the auditing components of the smart edge gateway. When events such as data path recovery due to smart edge gateway failures in the off-chain SDN network, or SDN controller failures leading to the takeover of the management domain by a guardian SDN controller, occur, all communication events can be comprehensively recorded.

From an auditing system efficiency perspective, important but low-volume audit data is directly stored on the security supervision chain, while high-volume audit data is stored in its higher-level semantics and hash value, while the audit data itself is stored off-chain in the IPFS network. Additionally, this paper proposes a delay-on-chain strategy for situations with high system load. This ensures the real-time nature of audit data storage, verifies data integrity through the security supervision chain, and guarantees

reliable storage via the IPFS network without a single point of failure.

Acknowledgments

This work was supported by the National Key Research and Development Program of China under Grant No. 2022YFB2702800.

References

[1] Ryno Adlam and Bertram Haskins. 2020. A Permissioned Blockchain Approach to Electronic Health Record Audit Logs. In *Proceedings of the 2nd International Conference on Intelligent and Innovative Computing Applications (ICONIC '20)*. Article 30, 7 pages. doi:10.1145/3415088.3415118

[2] Ashar Ahmad, Muhammad Saad, Mostafa Bassiouni, and Aziz Mohaisen. 2018. Towards Blockchain-Driven, Secure and Transparent Audit Logs. In *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous '18)*. 443–448. doi:10.1145/3286978.3286985

[3] A. Ahmad, M. Saad, L. Njilla, C. Kamhoua, M. Bassiouni, and A. Mohaisen. 2019. BlockTrail: A Scalable Multichain Solution for Blockchain-Based Audit Trails. In *IEEE International Conference on Communications (ICC)*. 1–6. doi:10.1109/ICC.2019.8761448

[4] Prabal Banerjee, Nishant Nikam, Subhra Mazumdar, and Sushmita Ruj. 2024. Cumulus: Blockchain-Enabled Privacy Preserving Data Audit in Cloud. *Distributed Ledger Technologies: Research and Practice* (2024). doi:10.1145/3672570 Just Accepted.

[5] G. Dong and X. Wang. 2020. A Secure IoT Data Integrity Auditing Scheme Based on Consortium Blockchain. In *5th IEEE International Conference on Big Data Analytics*. 246–250. doi:10.1109/ICBDA49040.2020.9101201

[6] Amit Kumar Dwivedi, Naveen Kumar, and Manik Lal Das. 2024. Edge Computing and Blockchain-Based Distributed Audit of Outsourced Dynamic Data. *Wireless Personal Communications* (2024). doi:10.1007/s11277-024-11094-3

[7] Danilo Francati, Giuseppe Ateniese, Abdoulaye Faye, Andrea Maria Milazzo, Angelo Massimo Perillo, Luca Schiatti, and Giuseppe Giordano. 2021. Audita: A Blockchain-based Auditing Framework for Off-chain Storage. In *Proceedings of the Ninth International Workshop on Security in Blockchain and Cloud Computing (SBC '21)*. 5–10. doi:10.1145/3457977.3460293

[8] Zhenyu Guan, Hanzheng Lyu, Haibin Zheng, Dawei Li, and Jianwei Liu. 2019. Distributed Audit System of SDN Controller Based on Blockchain. In *Smart Blockchain: SmartBlock 2019 (Lecture Notes in Computer Science, Vol. 11911)*, Meikang Qiu (Ed.). Springer, Cham, 21–31. doi:10.1007/978-3-030-34083-4_3

[9] N. Herbaut, C. Correa, J. Robin, and R. Mazo. 2021. SDN Intent-based Conformance Checking: Application to Security Policies. In *IEEE International Conference on Network Softwarization*. 181–185. doi:10.1109/NetSoft51509.2021.9492679

[10] Mohammad Belayet Hossain and P. W. C. Prasad. 2023. Securing Cloud Storage Data Using Audit-Based Blockchain Technology—A Review. In *Innovative Technologies in Intelligent Systems and Industrial Applications*, Subhas Chandra Mukhopadhyay, S. M. Namal Arosha Senanayake, and P. W. Chandana Withana (Eds.). Springer Nature Switzerland, Cham, 141–153. doi:10.1007/978-3-031-29078-7_14

[11] Xueping Liang, Sachin Shetty, Deepak Tosh, Charles Kamhoua, Kevin Kwiat, and Laurent Njilla. 2017. ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. In *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*. 468–477. doi:10.1109/CCGRID.2017.8

[12] J. C. López-Pimentel, O. Rojas, and R. Monroy. 2020. Blockchain and Off-chain: A Solution for Audit Issues in Supply Chain Systems. In *IEEE International Conference on Blockchain*. 126–133. doi:10.1109/Blockchain50366.2020.00023

[13] D. Malhotra, S. Srivastava, P. Saini, and A. K. Singh. 2021. Blockchain Based Audit Trailing of XAI Decisions: Storing on IPFS and Ethereum Blockchain. In *International Conference on COMmunication Systems & NETworkS*. 1–5. doi:10.1109/COMSNETS51098.2021.9352908

[14] Rahul Mishra, Dharavath Ramesh, Salil S. Kanhere, and Damodar Reddy Edla. 2023. Enabling Efficient Deduplication and Secure Decentralized Public Auditing for Cloud Storage: A Redactable Blockchain Approach. *ACM Transactions on Management Information Systems* 14, 3, Article 21 (2023), 35 pages. doi:10.1145/3578555

[15] W. Ren, Y. Sun, H. Luo, and M. Guizani. 2021. SILedger: A Blockchain and ABE-based Access Control for Applications in SDN-IoT Networks. *IEEE Transactions on Network and Service Management* 18, 4 (2021), 4406–4419. doi:10.1109/TNSM.2021.3093002

[16] Shuwen Sun and David Choffnes. 2022. Toward Flexible Auditing for In-Network Functionality. In *Proceedings of the 3rd International CoNEXT Student Workshop (CoNEXT-SW '22)*. 32–34. doi:10.1145/3565477.3569150

[17] Yuan Sun, Xing Zhang, and Mengyao Han. 2023. Research on the Application of Blockchain Technology in Big Data Auditing. In *Proceedings of the 2023 3rd International Conference on Robotics and Control Engineering (RobCE '23)*. 49–54. doi:10.1145/3598151.3598160

[18] J. Wang, S. Wang, L. Wang, W. Shao, S. Xu, and S. Zhang. 2022. A Blockchain and Edge Computing Based Public Audit Scheme for Cloud Storage. In *41st Chinese Control Conference*. 7466–7470. doi:10.23919/CCC55666.2022.9902871

[19] H. Yu, Z. Yang, S. Tu, M. Waqas, and H. Liu. 2022. Blockchain-Based Offline Auditing for the Cloud in Vehicular Networks. *IEEE Transactions on Network and Service Management* 19, 3 (2022), 2944–2956. doi:10.1109/TNSM.2022.3164549

[20] T. Yu, Y. Zhang, D. Chen, H. Cui, and J. Wang. 2019. Routing Loop Audit Mechanism Based on SDN. *China Communications* 16, 7 (2019), 96–108. doi:10.23919/JCC.2019.07.008

[21] Y. Zhao. 2024. Audit Data Traceability and Verification System Based on Blockchain Technology and Deep Learning. In *International Conference on Telecommunications and Power Electronics*. 77–82. doi:10.1109/TELEPE64216.2024.00020

[22] F. Zhou, X. Wang, L. Yin, L. Tao, and D. Chen. 2021. Research on the Application of Blockchain Technology: From the Perspective of Audit. In *International Conference on Intelligent Computing, Automation and Applications*. 581–584. doi:10.1109/ICAA53760.2021.00106