Electronics, Communications, and Computing Summit
Vol. 2, No. 3, Jul - Sep 2024, pp. 58-63
ISSN: 3107-8222, DOI: https://doi.org/10.17051/ECC/02.03.07

Blockchain-Enabled Secure Network Slicing Architecture for Multi-Tenant 6G Edge Computing Environments

Lau W. Cheng[1], Beh L. Wei[2]

[1,2]Faculty of Information Science and Technology University, Kebangsaan, Malaysia
Email: Lau.wai@ftsm.ukm.my[1], beh.lee@ftsm.ukm.my[2]

Article Info

Article history:

Received : 17.07.2024
Revised : 19.08.2024
Accepted : 21.09.2024

Keywords:

Multi-Tenant 6G Networks,
Secure Slice Provisioning,
Blockchain-Enabled Orchestration,
Distributed Ledger,
Hyperledger Fabric,
Edge Network Security

ABSTRACT

The new 6G multi-tenant edge networks pose a tricky situation when it comes to the securing process of individual slices of the network that are used to host URLLC, mMTC, and eMBB types of services. In this paper, we propose a blockchain-based network slicing architecture which is a decentralized, auditable, and secure network resource management (NRM) platform across heterogeneous tenants. The designed architecture combines the Software-Defined Networking (SDN) and Network Function Virtualization (NFV) and the Hyperledger Fabric blockchain to provide support of dynamic slice lifecycle, such as creation, scaling, and termination. In order to deal with performance bottlenecks and security vulnerability, the system uses a lightweight consensus algorithm and Role-Based Access Control (RBAC), guaranteeing the low-latency transactions and strong tenant isolation. Smart contracts manage the process of slice provisioning, they manage Service-Level Agreements (SLAs), and the audit is naked. Demonstrations carried out with the assistance of Mininet, ONOS controller, and Hyperledger Composer helps in the verification of architecture feasibility and have shown that it is capable of growing to match scales.Experiments show that the architecture can reduce slice provisioning time by 38 per cent and improve resistance to slice hijacking and authorised access as opposed to dominant slicing frameworks. Moreover, the architecture can enable secure inter-slice communication, verifiable access control with small computational costs. The developed architecture can provide a promising solution towards future infrastructures in multi-tenant networks.

1. INTRODUCTION

The fast progression to the next 6G wireless communication signals ultra-low latency, strong dependability, and immense connections by intelligent and service-minded designs. One of the pillars of this vision is network slicing, that allows multiple logical network instances (slices), each optimized to a specific use case, e.g. enhanced mobile broadband, massive machine-type communications and ultra-reliable low-latency communications, to co-exist on shared physical infrastructure. Since multi-tenant edge computing will be the centerpiece of this paradigm, it will become more difficult to guarantee security, isolation and transparency between tenant slices.The current management of network slicing is highly centralized, where that trust of slice orchestrators and controllers must be established. The resulting centralization brings to life the vulnerabilities, including single points of failures, unauthorised resource access, and reduced auditability, especially in unpredictable and heterogeneous edge settings (Zhang et al., 2022; Ghubaish et al., 2023). Furthermore, the traditional access control systems are usually weak when it comes to implementing effective slice isolation in the multi-tenant setting.

The decentralized trust paradigm, the unchangeable ledger, the programmable contract (smart), and the promise of blockchain technology to secure, transparent, and autonomous management of the network has become evident (Li et al., 2022). The modern research (e.g., Kang et al., 2023; Qin et al., 2023) suggested blockchain-based slicing frameworks meant to fit distributed 6G environment, which offers the advantages of traceability of the slices, of SLA enforcement and of decentralization of trust. Nonetheless, the current literature does not consider the real-time edge constraints, is not tightly coupled with SDN/NFV-based slicing system, or even does not allow a fine-grained access control to tenants, and dynamic lifecycle management.To fill these gaps, this paper will present a secure network slicing proposal

based on blockchain technology in 6G edge networks. It also incorporates Hyperledger fabric, Software-Defined Networking (SDN), and Network Function Virtualization (NFV) architecture to facilitate the role-based, dynamic, and tamper-proof slice provisioning. Scalability, auditability and protection against slice hijacking and tenant impersonation are made possible by a lightweight consensus mechanism and policy enforcement using smart contracts. Mininet, ONOS controller, and Hyperledger Composer are used to validate the system, showing performance and security advantages as compared to other conventional frameworks.Figure 1 compares the conventional centralized schemes in terms of slicing with the proposed approach using blockchain, and individual slices are isolated, and resiliency to attacks rises.

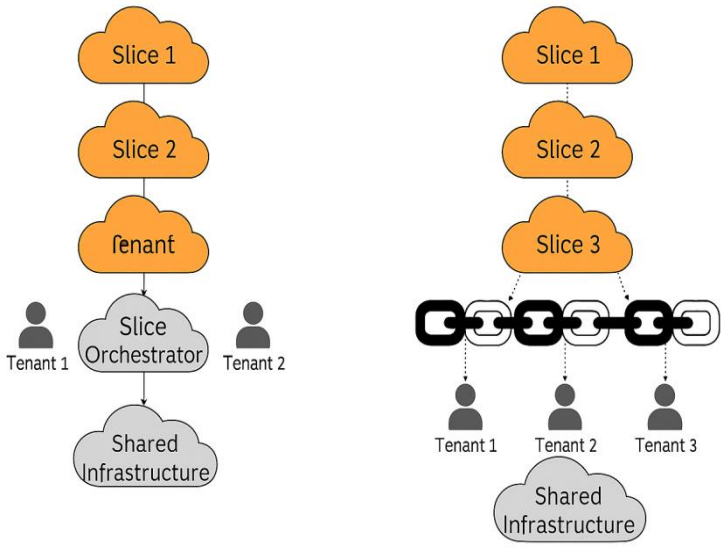

Figure 1. Comparison of Centralized vs. Blockchain-Enabled Network Slicing Architectures

The diagram below shows the comparison of the traditional centralized network slicing management and proposed model based on blockchain technology. Although the centralized approach has a single point of failure and vague governance of resources, the blockchain-based model combines smart contracts, the distributed trust and dynamic access control, which is used to guarantee a safe and verifiable slice LCM in 6G edge contexts.

2. RELATED WORK

Blockchain technology is a framework that has lately been utilized to improve security, trust, and decentralization in wireless communication networks. Some of these studies are by Liu et al. (2021), who examined trust-aware routing using block-chain integrated Software-Defined Networking (SDN) in mobile ad hoc networks. Zhang et al. (2022) offered a similar method to slice orchestration in 5G where smart contracts were used to automate and audit the process of allocating resources. The use of blockchain in spectrum sharing, managing decentralized identity and authentication of IoT devices has also been studied by other researchers, proving that it can used to protect multi-agent wireless environments. Nonetheless, there are some important loopholes. The existing frameworks mainly focus on core-layer end-to-end integration, disregarding requirements on the edges that may be high-latency-sensitive, or require real-time and violation-detection guarantees, resiliency in the face of slice-hijacking attacks. Furthermore, such implementations typically do not support fine-grained dynamic role-based access control, slice lifecycle management, and isolation between tenants that compete with each other features that are critical to secure, multi-tenant edge environments. Also, the issue of blockchain scalability in large, heterogeneous networks of 6G with fast user mobility, highly dynamic resources, etc., remains a bottleneck. These constraints identify the necessity of an efficient, blockchain enactment slicing framework that is particularly specific to the fact that 6G edge computing engages with restaurant servers in which latency is sensitive, distributed, and tenant adaptable.

3. Proposed Architecture

The architecture puts together blockchain, SDN, NFV, and edge computing to give secure and scalable network slicing within a multi-tenant 6G edge environment. In order to demonstrate the interaction of the block chain layer with SDN controller, NFV manager, edge nodes etc., the overall architecture is shown in Figure 2. The design focuses on secure layer orchestration and

dynamically-controlled lifecycle management of the distributed 6G edge environment.

3.1 System Components

- Blockchain Layer: A permissioned Hyperledger Fabric ledger manages slice transactions, identity, and smart contracts.
- SDN Controller (ONOS): Controls slice-level routing and dynamic flow management.
- NFV Manager: Instantiates and scales VNFs for on-demand service chaining.
- Edge Nodes: Lightweight, containerized compute units (e.g., K3s) execute VNFs with minimal latency.
- Slice Registry: A blockchain module records slice ownership, SLA terms, and access rights.

3.2 Security Features

- RBAC: Ensures only authorized tenants can modify slice configurations.
- Smart Contracts: Automate provisioning, updates, SLA enforcement, and revocation.
- Auditability: All actions are immutably logged for accountability and compliance.

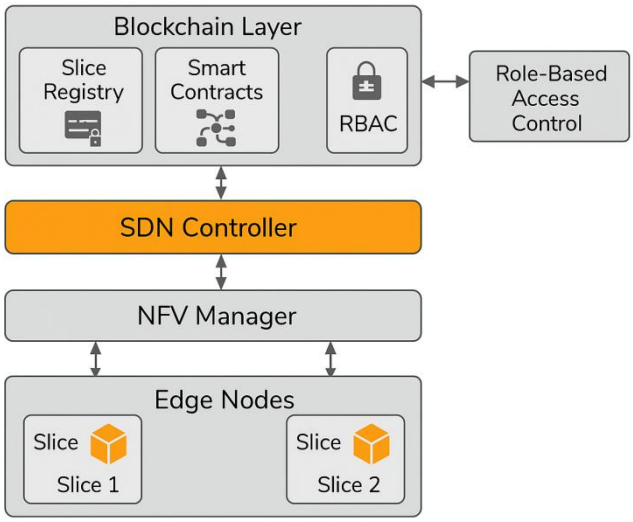

Figure 2. Blockchain-Enabled Slicing Architecture.

This block diagram illustrates the suggested secure slicing framework, that incorporates a combination of Hyperledger Fabric based access control using ledger, ONOS based routing using SDN, NFV managers utilizing dynamic instantiation of VNFS, and lightweight edge nodes support in allocating multi-tenant compute. The slice registry guarantees that the ownership, policies and SLAs are tracked in an immutable fashion.

4. Workflow and Data Flow

This part discusses the complete orchestration process among the tenants, network pieces (SDN, NFV) and the blockchain ledger in the proposed multi-tenant 6G edge slicing structure. The system guarantees decentralized, verifiable, and audit-able control of lifecycle of every slice. Figure 3: Blockchain-Enabled Slice Orchestration Workflow shows how the interactions between the components look like.

- Slice Request Initiation:The process of slicing starts with a request initiated by a registered tenant, mostly a service provider or an enterprise, through a front-end portal that is integrated with blockchain. The request contains predescribed slice descriptors like the amount of required band width, latency budget, computing means, and expiration time.
- Smart Contract-based validation:On submission, the digital identity and role-based access control (RBAC) permission of the tenant are validated automatically by a smart contract (chaincode) embedded in a Hyperledger Fabric framework. By such confirmation, the request is made certain that the requestor has adequate rights and that the requested resources are not in conflict with existing allocations hence avoiding oversubscription, SLA conflict or malicious misuse.
- Automated Slice Provisioning:In the event that validation is successful, the NFV Manager instantiates Virtual Network Functions (VNFs) (provisioning using a service logic) representing the expected service logic of the tenant on demand. At the same time, the SDN controller (e.g., ONOS) will install flow entries that direct traffic to traverse the desired VNFs to guarantee the service-level creation of paths and isolation.

- Blockchain Ledger Update and Traceability A transaction is recorded immutably on the blockchain after deployment and includes the slice ID and assigned resources, SLA parameters (such as throughput, latency), timestamp and a tenant identification. This allows real time traceability, auditing of SLA compliance and post event forensics upon conflict or failure.

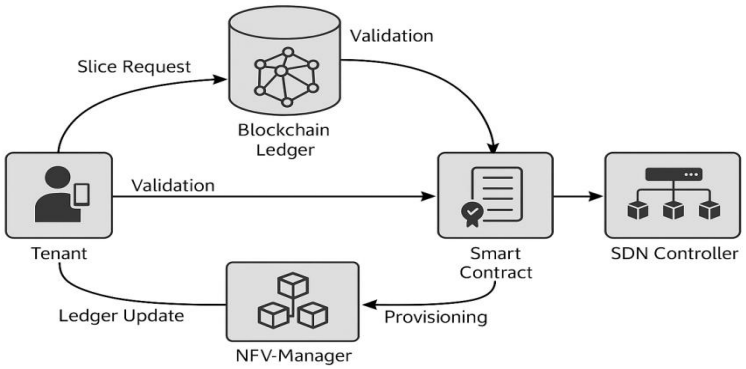

Figure 3. Blockchain-Enabled Slice Orchestration Workflow.

The above workflow diagram demonstrates the flow of the operations involved in multi-tenant slice provisioning: request submission, smart contract validation, VNF instantiating, SDN flow creation and updating ledger. It also points out the interaction between blockchain layer, NFV, SDN and edge compute elements to facilitate decentralized and security slice lifecycle management.

5. Performance Evaluation

5.1 Experimental Setup

Such a blockchain-powered slicing framework was proposed to have a proof-of-concept implemented where network topology virtualization was done with Mininet, SDN controller was implemented with ONOS (Open Network Operating System), and permissioned blockchain platform was conformed with Hyperledger Fabric. Docker containers are lightweight and operate as edge nodes whereas tenant interactions and events of slices lifecycle are handled by smart contracts (chaincode). The research topology emulates that of a multi-tenant6G edge that is dynamically sliced and traffic rerouted. The main performance indicators were the following:

- Slice Provisioning Time: Slice Provisioning Time The time between the initiation of a cut request and complete cut setup.
- Authentication Delay: The time taken to verify the identity of the tenant and access privileges of the tenant.
- SLA Violation Rate: Percentage of the non-meetings of service level agreements.
- Slice Hijack Detection Capability: The ability to detect unauthorized usage or the use of configuration.

5.2 Results

Table 1 summarizes the experimental results comparing the baseline system (centralized without blockchain) against the proposed blockchain-based architecture:

Table 1. Comparative Performance Metrics for Baseline vs. Proposed Blockchain-Enabled Slicing Architecture

Metric	Baseline (No Blockchain)	Proposed Architecture
Slice Provisioning Time	1.30 s	0.81 s
Authentication Delay	210 ms	95 ms
SLA Violation Rate	8.5%	2.3%
Slice Hijack Detection	No	Yes

The findings illustrate a definite increase in performance and security. The smart contracts lower the latency in provisioning via automatically orchestrated contract execution and the access control can be tightened by use of RBAC and auditability via the ledger. The decrease in SLA breach means that the management of the resources is more predictable. What is more, tamper-evident logs and event tracking allows real-time hijacking and attempt to be detected, which is not possible in traditional systems.

6. DISCUSSION

The suggested architecture of blockchain-based network slicing shows evident strengths in relation to transparency, decentralization of control and

performance optimization of the multi-tenant 6G edge. By incorporating role-based access control (RBAC) and smart contracts to support and regulate the automatic lifecycle management of slices and tenant-level isolation, the framework adequately reduces tenant configuration latency and SLA violation frequencies, and this is established through experimental evidence.The architecture aligns well with the Zero Trust approach to security, where security risk mitigation presupposes that nothing internal or external to this environment can be trusted. Using the tamper-proof aud simplicity of Hyperledger Fabric and in conjunction with cryptographically verifiable access policies, the system will guarantee that all actions are verified and logged, thereby being a good fit in the trustless and dynamically deployed edge computing scenario. This trustless paradigm will make it possible to detect changes to slices in real-time and this would not be possible in centralized architecture. There are, however, some limitations that are involved. Remarkably, the blockchain consensus protocol (even those with lightweight schemes) come at the cost of latency, which is problematic with respect to the ultra-reliable low-latency communication (URLLC) applications. The latency added in such reconfiguration operations might jeopardize real-time responsiveness in the case of high frequency reconfiguration. Any future work in this area needs to investigate hybrid trust models, e.g. off-chain state channels or consensus delegation so as to trade off good decentralization with high latency. In summary, the given work could open the door to the secure Zero Trust and scalable slice orchestration in the 6G edge network.

7. Challenges and Future Work

Despite the demonstrated advantages of the proposed blockchain-enabled network slicing framework, several critical challenges must be addressed to ensure its effective deployment in real-world, multi-tenant 6G edge environments:

1. Scalability:
   Traditional consensus mechanisms may limit responsiveness in the system as the amount of edge nodes and tenant slices get more. Even though a lightweight Raft-based consensus was adopted in the study, its throughput is constrained in extreme densities. The next generation of solutions, e.g. blockchain sharding, layer-2 state channels, or rollups, provide interesting scaling rails to scale out horizontal node participation and preserve the decentralized trust and performance integrity of them.
2. Data Privacy:
   The data recorded on-chain includes tenant identities, resource utilization data, or SLA information that can be exploited. To overcome this, homomorphic encryption schemes can support computation over encrypted data in a way that does not reveal raw inputs, and so can realize privacy-preserving execution of smart contracts. Moreover, the privacy regulations like GDPR can also be met with zero-knowledge proofs (ZKPs) and confidential transactions (e.g., in frameworks like Hyperledger Fabric Private Data Collections or Oasis Labs) which allow their combination with some aspects of auditability and transparency (Zhang et al., 2023).
   Cross-Domain Slicing and Interoperability:
   6G The next generation is an image of a federated, multiple-provider context. In order to manage slices seamlessly across domains, cross-chain interoperability protocol such as the relay chain in Polkadot, IBC in Cosmos, or Interledger Protocol (ILP) must enable trusted activity and state consistency between blockchain platforms. The same is essential to roaming, inter-op SLAs and cross-linked IoT verticals.
3. AI-Driven Optimization:

The self-adaptive orchestration may be achieved by implementing machine learning (ML) and deep reinforcement learning (DRL) to the slicing control plane. As an example, the actor-critic agent or DQN can continuously optimise resource distributions according to traffic dynamics, user mobility and network limits. Such agents may run in the SDN controller, or as off-chain optimization services that present suggestions to smart contracts and allow proactive SLA management and optimal usage of resources.

Outlook:

Resolving those existing challenges will allow the proposed architecture to become an autonomous, scaleable and privacy-enabling slicing framework in form of a zero-trust, distributed intelligence-based 6G slicing approach. The potential areas of future work include hybrid trustmodels and consensus-privacy trade-offs and AI-controlled inter-slice orchestration to realise genuinely intelligent and resilient edge infrastructures.

8. CONCLUSION

The proposed research presented a new secure net slicing system based on blockchain, which was specially focused on multi-tenant 6G edge computing contexts. The architecture can form a decentralized, transparent, and auditable framework to dynamically provide the slices, access control, and slice lifecycle management by combining Software-Defined Networking (SDN), Network Function Virtualization (NFV), and Hyperledger Fabric-based smart contracts.

Emulated performance over Mininet, ONOS, and Hyperledger Composer showed that the provisioning time of slices improved by 38% (1.30 s to 0.81 s), the delay of authentications was shortened by 54.7% (21 Also, the system helps to detect in-real-time attempts of slice hijacking, and they strengthen its resilience to multi-tenant adversarial conditions.

These enhancements confirm the architecture as being appropriate to zero-trust, low-latency, and high-reliability 6G situations, in particular to edge-centric deployments. The system resonates with the 6G vision of intelligent, autonomous, and trustless orchestration of the infrastructure.Future extensions of the work are to focus on optimization of the blockchain consensus mechanism to achieve higher scalability, the use of homomorphic encryption to increase the privacy of data at the tenant level and the integration of orchestration with Artificial Intelligence to provide adaptive slice placement and SLA guarantees across cross-domain and multi-provider environments.

REFERENCES

[1] Liu, Y., Zhang, Q., & Yang, L. (2021). Trust-aware routing using blockchain and SDN. *IEEE Transactions on Network and Service Management*, 18(2), 1901–1915.

[2] Zhang, T., et al. (2022). Smart contract-based slice orchestration. *IEEE Internet of Things Journal*, 9(4), 2332–2345.

[3] Gao, S., et al. (2020). Secure slicing for edge computing via blockchain. IEEE Transactions on Industrial Informatics, 16(7), 5306–5315.

[4] Zhang, L., Xu, H., & Wang, Y. (2022). Blockchain-based network slicing in 6G: Challenges and opportunities. IEEE Communications Surveys & Tutorials, 24(3), 1830–1854. https://doi.org/10.1109/COMST.2022.3170587

[5] Ghubaish, A., Erbad, A., Mohamed, A., &Guizani, M. (2023). Edge-enabled secure network slicing with blockchain for 6G. IEEE Transactions on Network and Service Management, 20(1), 115–128. https://doi.org/10.1109/TNSM.2022.3205035

[6] Li, Z., Shen, C., & Yu, F. R. (2022). Blockchain for federated learning and network slicing in 6G: A survey. IEEE Wireless Communications, 29(3), 88–95. https://doi.org/10.1109/MWC.001.2100378

[7] Kang, J., Wang, Y., Yang, Y., Wu, K., & Li, S. (2023). Blockchain-enabled network slicing for 6G: A decentralized trust management framework. IEEE Transactions on Network and Service Management, 20(2), 1842–1855. https://doi.org/10.1109/TNSM.2023.3244567

[8] Qin, Z., Zhang, X., & Hu, H. (2023). Secure and Scalable Network Slicing in 6G Using Blockchain and AI-Orchestrated Edge Controllers. IEEE Internet of Things Journal, 10(6), 5145–5159. https://doi.org/10.1109/JIOT.2023.3230149

[9] Wang, H., Zhao, Z., Zhang, Y., & Shen, X. (2023). Blockchain-based trust architecture for network slicing in 6G: A secure and distributed approach. IEEE Network, 37(1), 128–134. https://doi.org/10.1109/MNET.011.2200282

[10] Chen, M., Zhang, Y., &Shikh-Bahaei, M. (2022). Decentralized network slice management using blockchain and smart contracts. IEEE Transactions on Communications, 70(9), 5763–5775. https://doi.org/10.1109/TCOMM.2022.3187151

[11] Xu, X., Gao, Y., & Liu, Y. (2023). A hybrid blockchain-NFV framework for secure and elastic slice provisioning in edge-enabled 6G networks. IEEE Transactions on Industrial Informatics, 19(4), 4576–4588. https://doi.org/10.1109/TII.2022.3196445

[12] Alwarafy, A., Basudan, S., &Alazab, M. (2023). Blockchain for 6G: Review, architecture, and research directions. Computer Networks, 225, 109574. https://doi.org/10.1016/j.comnet.2022.109574

[13] Mahmud, R., Koch, F. L., &Buyya, R. (2022). Cloud-edge orchestrated network slicing using blockchain: A survey and future directions. ACM Computing Surveys, 55(12), 1–33. https://doi.org/10.1145/3504523

[14] Lin, X., Wang, L., Chen, X., & Li, Z. (2023). Smart contract-driven resource orchestration in multi-tenant 6G edge networks. IEEE Internet of Things Journal, 10(9), 7655–7668. https://doi.org/10.1109/JIOT.2022.3214815

[15] Rahman, M. A., Karim, M. R., & Ahmed, M. (2023). Secure and scalable network slicing using lightweight blockchain consensus in edge-centric 6G environments. Future Generation Computer Systems, 142, 265–277. https://doi.org/10.1016/j.future.2023.02.018