Enhancing Security in Software-Defined Networks using Blockchain Smart Contract

A thesis submitted in part fulfillment of the requirements for the degree of

Doctor of Philosophy

by

Birglang Bargayary

Registration No. TZ189349 of Year 2018

School of Engineering

Department of Computer Science and Engineering

Tezpur University, Tezpur - 784028

Assam, India

September 2025

CHAPTER 7

Conclusion and Future Directions

This thesis has made significant strides in enhancing the security, reliability, and integrity of Software-Defined Networking (SDN) through a series of carefully designed contributions. Our work addresses critical challenges in SDN, particularly in ensuring flow rule integrity, mitigating single points of failure, securing cross-domain interactions, and authenticating users and devices in SDN-IoT environments.

7.1 Research Findings

The following are the key findings of this research work:

a) By leveraging blockchain technology, we developed a secure and decentralized mechanism for verifying and maintaining the accuracy of flow rules through a specialized Blockchain Agent. The experimental studies validate the potential of our work and performance analysis shows that the proposed method can significantly reduce the execution time, transaction cost, and delay incurred due to the flow verification compared to BlockFlow [53], FRChain [101], and BlockSDSec [16]. This is because our method re-installs only the affected flow rules when a modification attack occurs. Further, the verification task can go on even if the controller goes offline. However, the proposed method is designed for single controller architecture which is a limitation of our work.

b) Our work further advances the reliability of SDN networks by introducing a distributed controller architecture designed to avoid the vulnerabilities associated with a single point of failure. By implementing a consensus-based approach, where more than one-third of the controllers must agree on the status of the master controller before declaring a failure, we have significantly enhanced the fault tolerance of the SDN control plane. It ensures that a single compromised controller or a minority of controllers cannot disrupt the network by falsely declaring the master controller as failed. Overall, the proposed architecture ensures increased resilience by incorporating a mechanism that dynamically selects the equal controller with optimal performance as a master controller in the event of failure, thus minimizing disruptions and optimizing network performance.

c) We further enhance the security of SDN flow rules on cross-domain SDN environments by developing a blockchain-based cross-domain proposal verification system. This system allows for secure and efficient verification of flow proposals across multiple administrative domains by following multi-stage security. Further, the security analysis indicates that the proposed adaptive policy mechanism enhances security by isolating the rogue controllers from influencing the voting decision for proposal verification. Further, it also significantly reduces the latency during repeated attacks on the system.

d) Finally, we proposed a blockchain-based authentication scheme that enhances the security of user and device authentication processes. A digital token is used to identify the users accessing a particular device on the SDN-enabled IoT network. The experimental results showed that the proposed method is effective in identifying the users through the blockchain token and can control unauthorized users from accessing the network resources. Therefore, this approach not only provides a scalable solution for authenticating a large number of devices but also ensures that the identities and access permissions of users and devices are securely managed and verifiable.

7.2 Limitations

Incorporating blockchain technology into our work offers several advantages, particularly in enhancing security and providing a decentralized framework for managing network operations. However, it is essential to acknowledge that this integration also brings inherent limitations, both from security and complexity perspectives.

a) **Smart Contract Vulnerabilities:** Although our solutions employ smart contracts for automation, these contracts are susceptible to bugs and vulnerabilities, which could be exploited if not carefully designed and audited. A compromised smart contract could lead to unauthorized access, incorrect flow rule enforcement, or even disruption of network services.

b) **Immutability Concerns:** The immutability of blockchain, while a strength in many respects, can also be a limitation. Once data is recorded on the blockchain, it cannot be altered or deleted. In the context of SDN, if erroneous flow rules or misconfigurations are logged on the blockchain, they could persist, potentially leading to prolonged network disruptions or security vulnerabilities until corrective measures are implemented.

7.3 Future Directions

Further work could explore on designing more sophisticated fault-tolerant algorithms to enhance the robustness of the distributed controller architecture. Additionally, we could integrate machine learning techniques for predictive failure detection and dynamic load balancing among controllers could further improve network reliability. Future research could also explore the use of advanced cryptographic techniques, like zero-knowledge proofs, to enhance the privacy and security of cross-domain transactions. Given the potential vulnerabilities in smart contracts, future research should focus on developing tools and methodologies for formal verification and secure coding practices. This would ensure that the smart contracts used in SDN environments are robust, secure, and free from exploitable bugs.

In conclusion, this thesis presents innovative solutions to some of the most pressing challenges in SDN, with a particular focus on security and reliability. The integration of blockchain technology across various layers of the SDN architecture has demonstrated its potential to transform the way networks are managed and secured. As the field of SDN continues to evolve, the contributions made in this work lay a strong foundation for future research and practical implementations, paving the way for more secure, reliable, and scalable network infrastructures.