Blockchain Enabled SDN Framework for Security Management in 5G Applications

Debashis Das*
Computer Science and Engineering
University of Kalyani
Kalyani, West Bengal, India
debashisdascse21@klyuniv.ac.in

Sourav Banerjee
Computer Science and Engineering
Kalyani Government Engineering College
Kalyani, West Bengal, India
mr.sourav.banerjee@ieee.org

Kousik Dasgupta
Computer Science and Engineering
Kalyani Government Engineering College
Kalyani, West Bengal, India
kousik.dasgupta@gmail.com

Pushpita Chatterjee
Electrical Engineering and Computer Science
Howard University
Washington, DC, USA
pushpita.c@ieee.org

Uttam Ghosh
Department of CS and DS
Meharry Medical College
Nashville, TN, USA
ghosh.uttam@ieee.org

Utpal Biswas
Computer Science and Engineering
University of Kalyani
Kalyani, West Bengal, India
utpal0172@gmail.com

ABSTRACT

Fifth-generation (5G) wireless networks are now operational to deploy all over the world. The technology of 5G's objective is to link heterogeneous machines and devices with significant improvements high quality of service (QoS), internet bandwidth, and improved system throughput to enable several upright applications. Despite all these benefits that 5G will provide, still, significant issues need to be resolved, such as decentralization, transparency, and risks associated with data interoperability, network privacy, and security vulnerabilities. Modern networks link an enormous number of devices to the Internet, and in this complicated situation, the use of BC and SDN has been effectively advocated to assure security, privacy, and secrecy. This study offers a blockchain-enabled SDN framework for securing transactions that makes use of Software Defined Network (SDN) and Network Function Virtualization (NFV) to overcome these issues. The proposed framework can address the man-in-the-middle attack between control and data plane in SDN networks. A controller authentication scheme is provided using smart contracts. Smart contracts automatically authenticate the SDN controller to increase the efficiency of controller verification. The communicated data can also be authenticated using smart contracts. The proposed framework can enhance network transparency, data security, and user privacy. Each SDN controller can access verifiable data using the proposed framework.

CCS CONCEPTS

• **Security and privacy → Tamper-proof and tamper-resistant designs**; **Trust frameworks**; • **Networks → Routers**.

ICDCN 2023, January 4–7, 2023, Kharagpur, India

ACM ISBN 978-1-4503-9796-4/23/01…$15.00
https://doi.org/10.1145/3571306.3571445

KEYWORDS

blockchain, distributed SDN, 5G network, blockchain-enabled SDN, wireless communication, smart contract

ACM Reference Format:
Debashis Das, Sourav Banerjee, Kousik Dasgupta, Pushpita Chatterjee, Uttam Ghosh, and Utpal Biswas. 2023. Blockchain Enabled SDN Framework for Security Management in 5G Applications. In *24th International Conference on Distributed Computing and Networking (ICDCN 2023), January 4–7, 2023, Kharagpur, India.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3571306.3571445

1 INTRODUCTION

Globally, the adoption of 5G mobile networks is anticipated to alter several industries and have a significant impact on consumers and other business leaders. Upcoming 5G services' objective is to provide a customized and intelligent provision of essentials, making it possible for nearly all parts of human activity to be connected to communication networks to meet the continually growing demands of network congestion and digital services [12]. Several underlying wireless technologies, including Software Defined Networking (SDN) have been suggested to support eventual 5G networks [5]. However, as the capability, performance, and scalability of 5G cellular modems quickly expand new security concerns such as network reliability, data integrity, and privacy surface [6].

Future 5G technologies are supporting emerging service delivery models that have indeed from security problems, as depicted in Figure 1. 5G wireless networks will be ubiquitous, decentralized, and service-oriented, in contrast to current cellular networks . Security management in 5G is challenging because of the diversity and quantity of connected devices [2].

The sustainable turn of technologies like IoT data collection, driver-less vehicles, unmanned aerial vehicles (UAVs), and deep learning depends on the security components of data integrity, autonomy, and openness in the 5G/6G future (FL). Blockchain is the most promising solution for its intrinsic features for 5G networks [3]. 5G needs blockchain to make its services widely available.

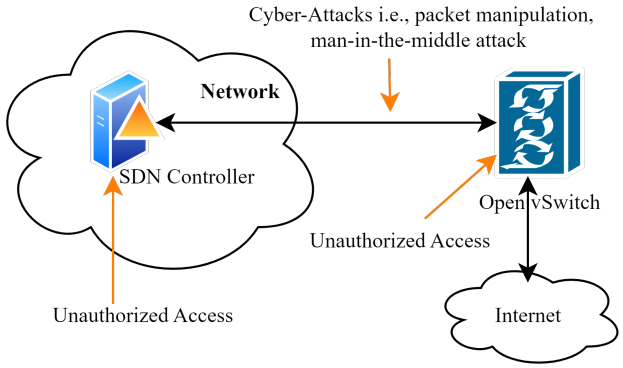

Figure 1: Possible Security vulnerabilities in SDN architecture

Blockchain is a distributed ledger system from a technical perspective, and it was first utilized as an accessible shared ledger for banking transactions using the cryptocurrency Bitcoin. Blockchain is essentially a decentralized, open, and immutable database. It is designed based on a P2P communication network where users may independently manage transaction information without being governed by a particular centralization [11].

Blockchain technology is particularly attractive because of its distributed, permanent, transparent, and completely fully decentralized database storage capacity, which significantly boosts information security and cut down on operating costs [16]. The rapid growth and adoption of blockchain as a technological breakthrough are paving the way for the next generation of commercial and financial businesses.Due to its inherent superior capabilities, blockchain may be linked with 5G ecosystems to boost mobile networks and services [13]. By spawning cutting-edge applications for ubiquitous computing, reliable evidenced preservation, and cognitive database administration, it is also envisaged that blockchains would significantly contribute to achieving the possibilities of 5Mobile communications.

Emerging solutions like blockchain (BC) and software-defined networking (SDN), which have recently found application use in a variety of P2P applications, are getting popularity in the academic world. The combination of blockchain with 5G is also projected to enable innovative telecommunication apps. In such a case, interconnectivity and resource wireless connections with high information rates and low delays would be provided by the 5G infrastructure. However, it presents concerns about secure communication and subnetwork trust. Due to its irreversible and decentralized transaction accounting records, blockchain can provide decentralized mass communication with high security and dependability [14].

This paper presents a blockchain-enabled SDN architecture for enhancing the efficiency and security of 5G applications. SDN controllers are connected with the proposed blockchain network to enable unauthorized access detection and data security. SDN controllers can control the data plane in a distributed manner with a transparent and collaborative management system. The proposed framework gives more data security using automatic verification of data using smart contracts.

The remained of this paper is organized as follows. Section 2 provides a literature review of existing works. In section 3, importance of blockchain-enabled SDN is briefly described. Section 4 depicts the proposed framework. Section 5 provides future research direction. Finally, section 6 gives a conclusion and future work.

2 RELATED WORKS

The incorporation of SDN into a decentralized blockchain architecture was created by Gao et al. [4] to enhance the functionality of vehicular ad-hoc networks (VANETs) and to monitor destructive behavior inside the network. The authors proposed employing zero-knowledge evidence based on voting-based consensus procedures to use the blockchain to check and certify trustworthy SDN switches, detect anomalous switch requests, and identify deviant switch requests.

However, these programs depend on centralized cloud-hosted safety infrastructure to provide authentication and confidentiality mechanisms. Lu et al. [8] presented a distributed energy trading system for the Internet based on SDN and blockchain. The privacy and safety criteria for power buildings were met by their architecture, which also offered an adequate match for the transaction objects.

Houda et al. [1] presented an SDN-based architecture for intra-domain, cross-functional and cross-DDoS mitigation. Cochain-SC offers a high degree of accuracy in spotting fraudulent flows and leverages Ethereum's smart contracts to facilitate communication across SDN-based large-scale domains. They developed a decentralized framework to offer safe identification, registration, and administration of interactive IoT devices. The recommended strategy enables the rapid detection of IoT resources and on-demand, secure IoT network instantiation.

Luo et al. [9] have suggested incorporating decentralized blockchain into a multi-SDN decentralized control and data planes that increase the scalability and flexibility of SDN-based industrial IoT and manage the vast quantity of data created by manufacturing equipment. The authors suggested a deep reinforcing learning (DRL) strategy using a partially observable Markov decision process to improve system energy savings, packet size, and flexible resource distribution (POMDP). Using edge-cloud and SDN, Medhane et al. [10] created a blockchain-based system that provides essential elements, including continuing secrecy, authenticity, and dependability.

According to Tan et al. [15], electronic decentralized and blockchain-enabled provenience mechanisms are needed for the crowdfunding system in 5G-enabled smart cities. The system described in the proposal progressively moves through the following nine steps: initiation, task submission, task publishing, task receipt, method capitulation, method mediation, payment, task rollback, and service compensation. An automated smart contract runs each stage, and payments are delivered through blockchain. No independent central entities are engaged. According to Lee and Ma's research [7], a blockchain-based approach is employed to overcome the problem of the key derivation methodology's inability to manage comprehensive forwarding key separation. Blockchain uses a complex strategy with fully forward key segregation to handle the necessary transition to 5G. To do this, the author concentrated on 5G mobility management.

According to Yazdinejad et al. research [18], the author creates a blockchain-enabled, energy-efficient SDN controller architecture for IoT networks by clustering SDN controllers and leveraging

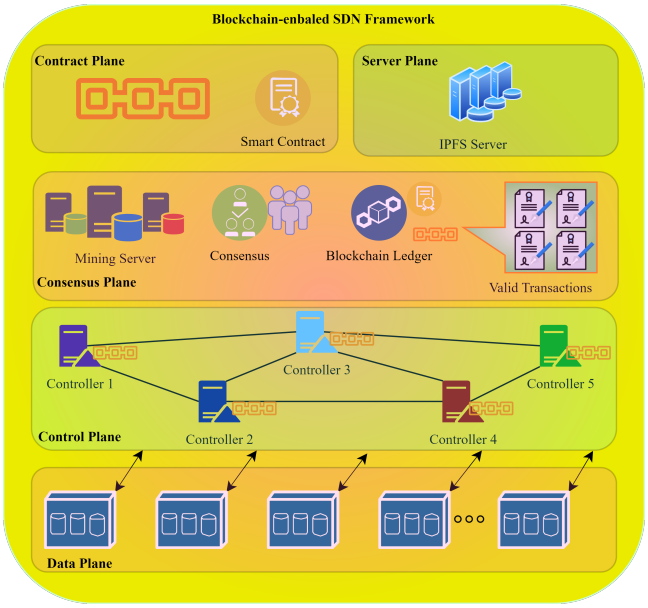

Figure 2: Blockchain-enabled SDN Framework

their routing protocol. The solution uses peer-to-peer (P2P) communication between IoT devices and SDN controllers on public and private blockchains to reduce POW and presents an authentication approach based on distributed trust for resource-constrained IoT devices.

3 CONSEQUENCE OF BLOCKCHAIN-ENABLED SDN FOR 5G APPLICATIONS

SDN allows for faster deployment of new internet protocol (IP)-based services and more efficient use of network resources. Blockchain technology makes it possible to overcome 5G networks' scalability, performance, reliability, and interoperability issues. There are a few number of challenges that need to be overcome before SDN can be utilised effectively in 5G and future networks. Figure 2 shows the blockchain-enabled SDN architecture.

3.1 Decentralization

Since there is just one SDN controller, it creates a single point of failure when it is compromised. The development of a distributed SDN architecture is required, especially when a secondary controller may regulate the internet flow of traffic. Scalability has similar top concerns to safety, integrity, and interoperability, and vice versa.

3.2 Scalability

Centralized or partially distributed controllers that connect to many network devices and deal with the data planes on several devices are used in SDN designs. There are more customers or participants active at once. The performance of deployment of SDN is more like a network operating system in terms of how it uses a different control and data plane design, which adds latency. In large area networks, this might result in significant delay and a decline in network performance, response, and processing times for controllers.

3.3 Security

Regarding security solutions, safeguarding the controller is essential. Security flaws might exist due to a lack of standards and regulations for software development. Network monitoring may result in significant expenses that have the potential to negatively impact the performance of 5G networks. Recently, blockchain has been employed in 5G networks that are virtualized to ensure security. BlockONet is an approach developed by [17] to enhance the connection and security of the 5G network. Blockchain on a cloud-RAN 5G network has two key benefits. Single-point failure bottlenecks are removed, dramatically enhancing system trust.

3.4 Consensus

The most effective platform for this range of dynamic, scattered, and heterogeneous 5G networks have shown to be blockchain. Additionally, it keeps track of all the transactions to ascertain the current market prices, assisting network operators and users. A deep reinforcement learning-based approach for permissioned content caching in edge networks can be developed using blockchain and SDN. As more base stations are built, proof-of-utility-based consensus (PoU) is advised as a means of agreement.

3.5 Trusted Communication

Software-Defined Networking (SDN) has already achieved significant interest over the past few years and has been considered the key foundation of potential 5G Mobile communications. SDN is an intelligent networking framework that anticipates enhancing the programmable macros and adaptability of connections. The isolation of the control and data planes from the network switches and the delivery of external data control through a rational currently dominates, permitting cooperative communication across various components of heterogeneous networks, which are the core ideas of SDN.

4 PROPOSED FRAMEWORK

This section provides the system overview of the proposed framework entitled blockchain-enabled SDN framework for 5G applications using smart contracts. It addresses the existing issues in SDN architecture, such as cyberattacks and unauthorized access to SDN controllers and switches. Figure 3 shows the system overview of the blockchain-enabled SDN framework for 5G applications. This suggested method facilitates safe information transfers across many SDN controllers by allowing them to interface with blockchain and communicate with one another. The specialized transfer keys to the controller can be used to share blockchain transactions and messages.

Each SDN controller has a unique transfer key obtained from blockchain technology and is used to send and receive data. A hierarchical structure built on a blockchain can successfully address the issue of scalability. When an SDN controller in a cell goes down, the system will govern that cell using another SDN controller in the network, where blockchain ledgers may be used to reach a consensus between SDN controller candidates.Thus, the use of blockchain in SDN holds up the prospect of doing away with intermediaries for identification, cutting transaction costs, and enabling universal accessibility for all individuals.

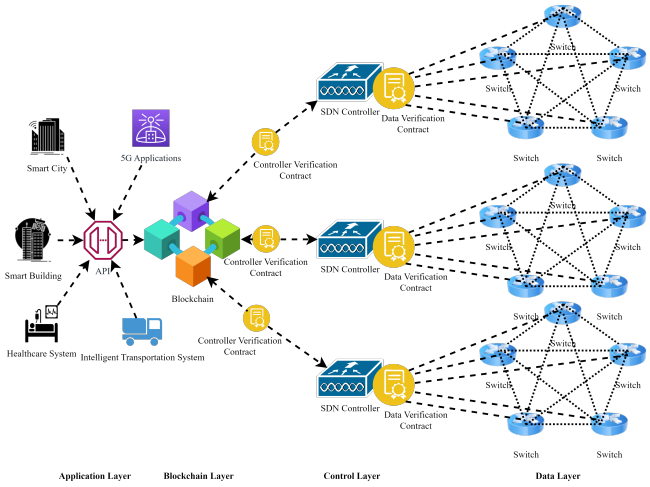

Figure 3: Blockchain-enabled SDN for 5G applications

In the proposed framework, underlying data forwarding is provided by the data plane and is software specified using the OpenFlow protocol. All of the controllers in the control plane are distributedly connected by blockchain and are located in various control domains. Smart contracts use the consistent data in the distributed ledger to perform the specific network function, and at the software level, each controller in the control plane is loaded with the identically distributed ledger maintained by the consensus plane. While the contract plane includes smart contracts to carry out autonomous network operations, the consensus plane provides multi-controller consensus for the pending-process services and puts the outcomes into a block data format on a distributed ledger.

This study offers a blockchain-based consensus mechanism that communicates with the SDN domain control layer to gather and synchronize data from various dispersed SDN controllers. Particularly, at the area control layer, data and links are gathered and delivered to the domain control layer, which runs on a distributed blockchain. Blockchain is used in distributed software-defined 5G applications to transfer model parameters from one domain to another domain controller in a transactional way.

The proposed framework has four layers, which are the data layer, control layer, blockchain layer, and application layer. These layers are described in the following:

4.1 Data Layer

The Data plane of SDN architecture is here the data layer. Data packets are transmitted in this layer. Data security is the primary security consideration in network applications. Thus, the security protocol is needed to secure transmitted data without hampering network controls and regulations. A secure authentication scheme is proposed to ensure data security using smart contracts in the proposed work. So, each transmitted data can be verified automatically in a short time. Each SDN controller has a unique identity, and each switch has a unique identity to identify them. So, smart contracts can identify the SDN controller and switch. Therefore, transactions of transmitted data can be traced by authorized authority. So, malicious activities can be addressed using this framework. Authentication, mobility, and data management are among the global policies that the SDN controller is in charge of, while the data plane implements the controller-defined policies.

Blockchain's irreversible and decentralized capabilities help record all 5G communications and foster confidence for the SDN-based 5G application to secure accurate message transmissions and prevent inauthentic messages. Furthermore, in SDN, security refers to data preservation in the data plane and control plane authentication. In this framework, blockchain can offer a decentralized security provisioning system solution.

4.2 Control Layer

The control plane in SDN architecture is here the control layer. Packet transmission regulations are controlled in this layer. Smart contracts are designed and developed by authenticated nodes that are connected to the blockchain network of the blockchain layer. SDN controllers are connected with the blockchain network and can control the packet flow rules as a part of smart contracts. Smart contracts' configuration and management are controlled in this layer. Figure 4 shows the P2P communication between blockchain and SDN controllers.A peer-to-peer network using SDN resources that is blockchain-secured to ensure that every transaction on SDN complies with regulations while maintaining high data interoperability. The suggested plan is capable of performing efficient authorized interactions between several 5G applications, securely transferring communicated data to many businesses and gadgets, and enhancing the general effectiveness of 5G applications.

4.3 Blockchain Layer

The blockchain layer represents a storage layer. All transactions are stored in this layer as a block in a blockchain ledger. Smart contracts are also stored in the blockchain. This layer is connected with the control layer using the northbound application programming interface (API). All the verification data will be stored here in secure storage using a block hash that can be generated using

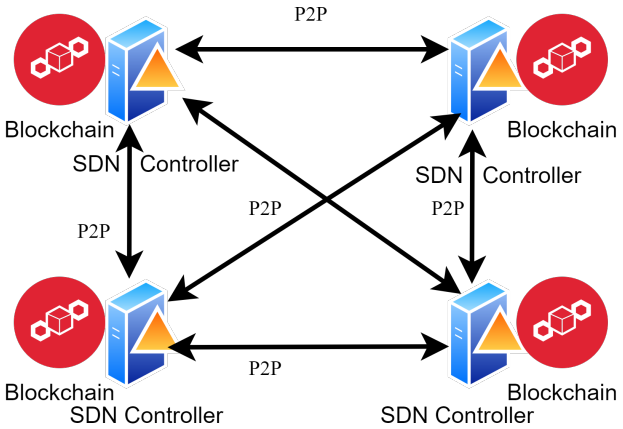

Figure 4: P2P communication between SDN controllers

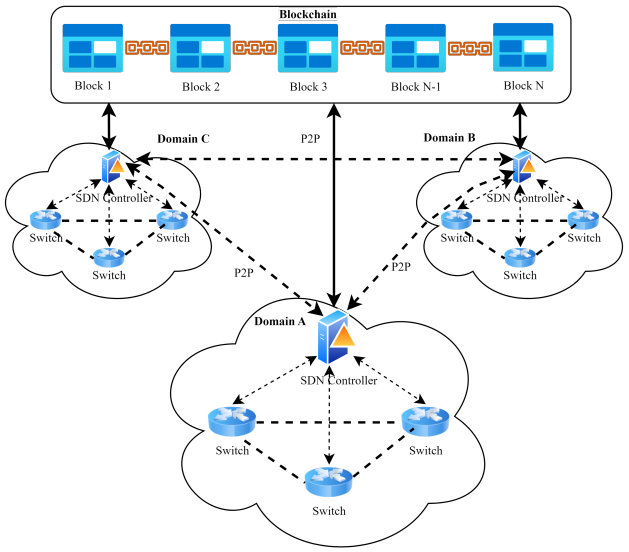

Figure 5: Blockchain-enabled access control in different SDN controllers

a cryptographic hash. All transactions are kept in each SDN controller. So, no one can violate the network rules and regulations. Figure 5 shows the access control among several SDN controllers using blockchain. As a key security mechanism, it offers immutable and incorruptible blockchain to address possible SDN threats such as unauthenticated access control, Denial-of-Service (DoS) assaults, SDN controller attacks, and flooding attacks.

The prposed framework generates a blockchain-based global trust evaluation system for SDN-based home network controllers. Using a condensed risk assessment scale, users may give isolated network slices the amount of trust they wish. The trust scores of users can be updated by SDN controllers, and scores can be evaluated via reports. Scores are then securely kept using blockchain in a tamper-resistant distributed way. Several security challenges can be resolved using the blockchain, including data integrity utilizing distributed ledgers and fault tolerance made possible by blockchain consensus.

4.4 Application Layer

The application layer is the frontend part of the proposed framework. This layer is connected with the blockchain layer through the user API, and users can access blockchain data. Several applications can be designed using the proposed framework. SDN controllers can show the packet flow using this API as they act as blockchain nodes. So, this layer can be an application-specific layer, where SDN controllers can communicate with open switches using blockchain and smart contracts securely.

5 FUTURE RESEARCH DIRECTIONS

5.1 Scalability

Transactions per second (TPS) is used to quantify how quickly transactions are accepted on a blockchain. The slow transaction speed of blockchain is a big worry for many businesses embracing the technology, notably 5G. Most current blockchain systems have a low transaction rate and are not compatible with 5G networks. Two elements dominate in determining the throughput of the blockchain. First, there are the consensus algorithms that decide how to decide to add the block. Second, the design of the blockchain. A private or consortium blockchain, which is most likely the case for 5G, is anticipated to achieve a better transaction rate than a public blockchain because of a regulated environment and fewer players in the transaction approval process. The utilization of such consensus methods in a dynamic, heterogeneous network with a high volume of transactions from various devices at different levels in the 5G network has to be further studied.

5.2 Security

Blockchain has several security vulnerabilities, even though it is widely acknowledged as a solution to several security problems in the 5G network. Consensus protocols, for instance, which make up the core of blockchain technology, are increasingly frequently the target of attackers. Additionally, the blocks can be altered if the attacker has control over more than 50% of the nodes in the blockchain network (also known as a 51% assault). Before being widely used, consensus algorithms need to have their security thoroughly evaluated. Additionally, the smart contract essential to blockchain's success may not be safe owing to deficient coding.

5.3 Resource management

Before a transaction is approved or refused on a blockchain, calculations must be performed on it. Consensus methods can be computationally demanding for this reason. As a result, it is not practical for all network nodes to take part in the transaction validation process. Due to the possibility that the necessary resource won't be made available in time, this circumstance may result in a bottleneck and decreased network performance.

Due to resource limitations, the 5G network needs an optimization framework that dynamically chooses the mining node in a permissioned network. Therefore, it is necessary to look at resource provisioning for computing in a 5G network to support a blockchain. In addition, not all nodes, particularly IoT devices, are capable of running blockchain. The network that has to be explored may require the best placement of specialized validating nodes to address this difficulty. The blockchain also needs the transaction to be broadcast for approval, which might result in a considerable overhead and increase network traffic.

5.4 Data Handling

5G networks allow data transmission between blockchain users on the edge, core, and mobile devices. To make judgments and actionable insights, this is crucial. Determining the types of data that will be kept on the blockchain and off-chain in the cloud is also crucial. Because blockchain can store a limited quantity of reference data. This issue must be resolved to guarantee compatibility and acceptance throughout the ecosystem.

5.5 Secure Environment

Since the launch of Bitcoin, several blockchain systems have become available. However, there isn't enough experimental research to say

if one platform is more suited than the other. This makes it difficult to implement a blockchain platform on 5G networks that can meet a variety of needs, including those related to performance, infrastructure costs, and data protection, among others. Without more experimental support, this problem cannot be solved. Therefore, research projects must be carried out by the blockchain research community to investigate and report on the appropriateness of various blockchain platforms for integration with 5G networks and beyond.

5.6 Storage and Network Management

Consensus on the blockchain takes a lot of overhead and processing resources. The network's bandwidth may be significantly used by this overhead. In some cases, there might not be enough resources to allow for timely consensus, which can lead to excessive latency. Some blockchain solutions call for the node to have a complete copy of the blockchain's transaction data, which is impractical for devices with limited capabilities. Some initiatives have been made in this regard. But for application in 5G and other networks, further testing and study are required. Blockchain offers the chance to create superior machine-learning models. Blockchain's ability to share data safely and securely will cause data from different silos to converge across many stakeholders. So, useful data-driven insights, predictions, and optimization will be produced. There have been various initiatives in this approach that reflect the possibility of combining blockchain technology and machine learning.

6 CONCLUSION AND FUTURE WORK

SDN is a modern architecture that separates the control and data plane to increase network performance and efficiency. It is a programmatically configured and centrally managed application in various industries. Regardless, several issues, like unauthorized access to the SDN controller and switches and cyber-attacks, can be possible in the SDN architecture. Therefore, we developed a blockchain-enabled SDN framework to address potential security vulnerabilities that can manipulate packet flow control over the network. Blockchain provides the distributed SDN framework with network transparency and data security. Due to its safe design principles, blockchain addresses fundamental security problems including, consistency, authenticity, trustworthiness, and accessibility in a decentralized way. The proposed authentication scheme enables trust among SDN controllers. It can verify blockchain nodes automatically to detect unauthorized access in the SDN architecture.

The proposed framework is designed for 5G applications. Here, blockchain and SDN can enhance the performance of 5G applications efficiently. Most of the 5G applications are based on centralized systems that can be harmful to sustainable applications. The proposed framework enhance the security and privacy of SDN's planes. Therefore, sustainable 5G applications can perform in a trusted manner in several network functionalities. This framework can resolve significant available issues by providing decentralization, transparency, and availability features. The transmitted data can also be verified using smart contracts. In the future, data flow analysis will be suggested in the data layer based on the network traffic to enhance control management and efficient packet flow. Event order also is maintained using the extended framework.

REFERENCES

[1] Zakaria Abou El Houda, Abdelhakim Senhaji Hafid, and Lyes Khoukhi. 2019. Cochain-SC: An Intra- and Inter-Domain Ddos Mitigation Scheme Based on Blockchain Using SDN and Smart Contract. *IEEE Access* 7 (2019), 98893–98907. https://doi.org/10.1109/ACCESS.2019.2930715

[2] Deborsi Basu, Vikash Kumar Gupta, Raja Datta, and Uttam Ghosh. 2021. Dynamic Cluster Based Control Plane Load Balancing in Large Scale vSDN-enabled 5G WAN. In *2021 IEEE 3rd PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS)*. 1–2. https://doi.org/10.1109/PhDEDITS53295.2021.9649455

[3] Konstantinos Christidis and Michael Devetsikiotis. 2016. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* 4 (2016), 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

[4] Jianbin Gao, Kwame Opuni-Boachie Obour Agyekum, Emmanuel Boateng Sifah, Kingsley Nketia Acheampong, Qi Xia, Xiaojiang Du, Mohsen Guizani, and Hu Xia. 2020. A Blockchain-SDN-Enabled Internet of Vehicles Environment for Fog Computing and 5G Networks. *IEEE Internet of Things Journal* 7, 5 (May 2020), 4278–4291. https://doi.org/10.1109/JIOT.2019.2956241

[5] A. Gupta and R. K. Jha. 2015. A Survey of 5G Network: Architecture and Emerging Technologies. *IEEE Access* 3 (2015), 1206–1232. https://doi.org/10.1109/ACCESS.2015.2461602

[6] D Hemanand, D. S. Jayalakshmi, Uttam Ghosh, A. Balasundaram, Pandi Vijayakumar, and Pradip Kumar Sharma. 2021. Enabling Sustainable Energy for Smart Environment Using 5G Wireless Communication and Internet of Things. *IEEE Wireless Communications* 28, 6 (2021), 56–61. https://doi.org/10.1109/MWC.013.2100158

[7] Han Lee and Maode Ma. 2020. Blockchain-based mobility management for 5G. *Future Generation Computer Systems* 110 (2020), 638–646. https://doi.org/10.1016/j.future.2019.08.008

[8] Xin Lu, Lingyun Shi, Zhenyu Chen, Xunfeng Fan, Zhitao Guan, Xiaojiang Du, and Mohsen Guizani. 2019. Blockchain-Based Distributed Energy Trading in Energy Internet: An SDN Approach. *IEEE Access* 7 (2019), 173817–173826. https://doi.org/10.1109/ACCESS.2019.2957211

[9] Jia Luo, Qianbin Chen, F. Richard Yu, and Lun Tang. 2020. Blockchain-Enabled Software-Defined Industrial Internet of Things With Deep Reinforcement Learning. *IEEE Internet of Things Journal* 7, 6 (June 2020), 5466–5480. https://doi.org/10.1109/JIOT.2020.2978516

[10] Darshan Vishwasrao Medhane, Arun Kumar Sangaiah, M. Shamim Hossain, Ghulam Muhammad, and Jin Wang. 2020. Blockchain-Enabled Distributed Security Framework for Next-Generation IoT: An Edge Cloud and Software-Defined Network-Integrated Approach. *IEEE Internet of Things Journal* 7, 7 (July 2020), 6143–6149. https://doi.org/10.1109/JIOT.2020.2977196

[11] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

[12] Dinh C. Nguyen, Pubudu N. Pathirana, Ming Ding, and Aruna Seneviratne. 2020. Blockchain for 5G and beyond networks: A state of the art survey. *Journal of Network and Computer Applications* 166 (2020), 102693. https://doi.org/10.1016/j.jnca.2020.102693

[13] Nisha Panwar, Shantanu Sharma, and Awadhesh Kumar Singh. 2016. A survey on 5G: The next generation of mobile communication. *Physical Communication* 18 (2016), 64–84. https://doi.org/10.1016/j.phycom.2015.10.006

[14] Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, and Mohammed Samaka. 2019. Security Services Using Blockchains: A State of the Art Survey. *IEEE Communications Surveys & Tutorials* 21, 1 (2019), 858–880. https://doi.org/10.1109/COMST.2018.2863956

[15] Liang Tan, Huan Xiao, Keping Yu, Moayad Aloqaily, and Yaser Jararweh. 2021. A blockchain-empowered crowdsourcing system for 5G-enabled smart cities. *Computer Standards & Interfaces* 76 (2021), 103517. https://doi.org/10.1016/j.csi.2021.103517

[16] Florian Tschorsch and Bjorn Scheuermann. 2016. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys & Tutorials* 18, 3 (2016), 2084–2123. https://doi.org/10.1109/COMST.2016.2535718

[17] Hui Yang, Yizhen Wu, Jie Zhang, Haowei Zheng, Yuefeng Ji, and Young Lee. 2018. BlockONet: Blockchain-based Trusted Cloud Radio over Optical Fiber Network for 5G Fronthaul. In *2018 Optical Fiber Communications Conference and Exposition (OFC)*. 1–3.

[18] Abbas Yazdinejad, Reza M. Parizi, Ali Dehghantanha, Qi Zhang, and Kim-Kwang Raymond Choo. 2020. An Energy-Efficient SDN Controller Architecture for IoT Networks With Blockchain-Based Security. *IEEE Transactions on Services Computing* 13, 4 (2020), 625–638. https://doi.org/10.1109/TSC.2020.2966970

Received 15 September 2022; revised 6 November 2022; accepted 6 November 2022