Original research article / Originalus mokslinis straipsnis
Vol. 1 No. 10 (2025): Gruodis

A Blockchain-Based Decentralized Security Management Model for 5G and SDN Networks

[1] Narmin Ahmedli

Accepted: 11.15.2025
Published: 12.03.2025
https://doi.org/10.69760/portuni.0110005

Abstract. The convergence of 5G networks and Software-Defined Networking (SDN) has introduced a new paradigm in secure communication management, yet traditional centralized security frameworks struggle to meet the demands of highly dynamic, device-dense environments. To address issues of scalability, reliability, and transparency, this study proposes a decentralized security architecture grounded in blockchain technology. The research integrates theoretical analysis with system modeling and comparative simulation to evaluate the model's effectiveness. In the proposed design, the SDN control layer is linked to a blockchain network, enabling decentralized authentication, authorization, and event auditing through smart contracts. Simulation outcomes indicate that blockchain-assisted control enhances identification and verification processes by approximately 25–30%, mitigates single-point-of-failure vulnerabilities, and significantly strengthens system-wide trust. By ensuring immutability, distributed trust, and robust operational security, the model provides a resilient framework for next-generation 5G–SDN infrastructures. The study's scientific and practical value lies in demonstrating how blockchain can establish a sustainable, transparent, and secure ecosystem for future communication networks.

Keywords: *Blockchain, 5G networks, SDN, decentralized security, trust management, smart contracts.*

1. Introduction

In the modern era, the digital transformation driven by advances in information and communication technologies (ICT) has affected virtually all spheres of society. In particular, fifth-generation mobile communication technologies (5G) and the Software-Defined Networking (SDN) paradigm are radically reshaping the architecture and management of global communication systems (Kreutz et al., 2015). Owing to high data transmission rates, ultra-low latency, and massive device connectivity, 5G plays a central role in the development of industrial automation, healthcare, education, logistics, artificial intelligence applications, and "smart city" ecosystems. SDN, by decoupling the control and data planes and implementing network control in software, significantly increases flexibility, programmability, and centralized visibility over network resources (Kreutz et al., 2015). The convergence of these two technologies—5G–SDN integration—constitutes the backbone of next-generation communication infrastructures.

[1] Ahmadli, N. I year Master's student of the Department of Electronics and Information Technologies, Nakhchivan State University. Email: nrminhmdli5@gmail.com. ORCID: https://orcid.org/0009-0002-2164-684X

1.1. Security Challenges in 5G–SDN Architectures

Despite their advantages, integrated 5G–SDN environments pose serious security challenges. In SDN architectures, the logically centralized controller becomes a critical dependency and potential single point of failure: if compromised or overloaded, the entire network may be affected. At the same time, 5G networks must manage an enormous number of heterogeneous users, devices, and services, which complicates the assurance of core security properties such as authentication, integrity of data flows, confidentiality, and trust management between entities.

Moreover, the inherently distributed nature of 5G services—spanning multiple domains, operators, and service providers—makes it difficult to establish and maintain robust trust relationships. Traditional security mechanisms, largely built around centralized identity management and certification authorities, are often unable to respond effectively to the scale, dynamism, and heterogeneity of 5G–SDN ecosystems. Attack detection may be delayed, correlation of events may be incomplete, and centralized incident handling can become a performance bottleneck. As a result, network resource management can become unstable, and response times to security threats may increase.

1.2. Blockchain as a Decentralized Trust Layer

Against this background, blockchain technology has emerged as a promising approach to mitigate these challenges. As a distributed ledger system, blockchain replaces the traditional centralized trust model with a consensus-based architecture in which data are stored in a transparent, immutable, and traceable manner (Wood, 2014). These characteristics make blockchain an attractive candidate for security management in multi-layered and distributed environments such as SDN-enabled 5G networks (Zhang et al., 2019).

Through blockchain, trust relationships between network components can be established without reliance on a single central authority. Identification, authentication, authorization, and event logging can be implemented via smart contracts that automatically enforce predefined policies. Recent studies have explored blockchain-enabled security frameworks for 5G–SDN networks and related scenarios (Al-Fuqaha et al., 2023; Kumar & Singh, 2022; Lin & Zhu, 2024; Zhang et al., 2019). However, many of these proposals remain largely conceptual or focus on specific use cases, and several open issues persist. These include the full integration of blockchain with the SDN control plane, the real-time enforcement of security policies, performance overheads, and the scalability of consensus mechanisms under 5G-level traffic and device density.

1.3. Problem Statement and Research Gap

The current landscape thus reveals a clear gap between theoretical potential and practical deployment. Existing solutions often address isolated aspects of security—such as access control, key management, or logging—without offering a holistic, operationally viable framework for decentralized security management in 5G–SDN networks. Questions remain regarding how blockchain can:

- be tightly coupled with SDN controllers without introducing unacceptable latency,

- support automated, fine-grained security policy enforcement across diverse 5G slices and services, and
- maintain high availability and resilience without compromising network performance.

These unresolved issues indicate the need for more comprehensive models that not only conceptualize but also operationalize blockchain-based decentralization of security management in 5G–SDN environments.

1.4. Aim and Contribution of the Study

In this context, the present study proposes a blockchain-based decentralized security management model tailored for integrated 5G–SDN architectures (Zhang et al., 2019). The central idea is to shift from a single-controller trust model to a distributed trust fabric in which security-relevant decisions and records are shared among network participants via blockchain. In the proposed approach, the SDN control layer is interconnected with a blockchain network, and critical operations—such as authentication, authorization, and security event monitoring—are automated and governed by smart contracts.

In such a system, trust is no longer concentrated at a single control node but is instead distributed across multiple validating entities, thereby reducing the risk of a single point of failure and enhancing transparency and accountability. The main objective of the model developed within this research is to increase the security and trust level of 5G–SDN networks while preserving, and where possible improving, performance and scalability.

From both a scientific and applied perspective, this approach can be considered an innovative direction for ensuring security in next-generation communication systems. It offers a conceptual and technical framework for building resilient, transparent, and decentralized security infrastructures that are better aligned with the demands of future 5G–SDN ecosystems.

2. Methodology

This research was conducted to investigate how security management in 5G and SDN architectures can be optimized through a blockchain-based decentralized approach in comparison with traditional centralized models. The study employed a combination of **theoretical analysis**, **system modeling**, and **comparative simulation** within an experimental–simulation design. A decentralized security architecture modeling the interaction between the SDN control layer and a blockchain network was developed and evaluated in a virtual 5G–SDN environment.

The **object of the research** is the security management environment of 5G networks, including the SDN controller layer and related security processes. The main network components—SDN controller, switches, user equipment (UE), and identification modules—were modeled to reflect realistic control and data-plane interactions.

2.1. Tools and Technologies

The following tools and technologies were used in the implementation and evaluation of the proposed model:

- **Mininet** – to build and emulate the SDN network topology.
- **ONOS or OpenDaylight SDN Controller** – to simulate the SDN control layer.
- **Hyperledger Fabric / Ethereum Test Network** – to create and manage the blockchain environment (Wood, 2014).
- **Python and Solidity** – to develop, deploy, and integrate smart contracts for security operations.
- **Wireshark and sFlow** – to monitor network traffic and analyze security-related events.
- **SPSS and SciPy** – to perform statistical analysis and measure performance differences between scenarios.

2.2. Experimental Design and Scenarios

The research was carried out in several structured stages:

1. **Baseline Model Construction**

   A classical centralized security model for integrated 5G–SDN networks was designed and implemented. In this configuration, authentication and authorization processes relied on centralized servers and controller logic.

2. **Blockchain Integration**

   A blockchain network (Hyperledger or Ethereum test environment) was instantiated and integrated with the SDN control layer at the API level, enabling bidirectional communication between the controller and the blockchain.

3. **Smart Contract Development**

   Smart contracts were designed for **authentication** and **authorization** mechanisms, automating identity verification, access control, and logging of security events.

4. **Scenario Definition and Testing**

   Two main scenarios were executed and compared:

   - **Scenario A:** Classical centralized SDN management.
   - **Scenario B:** Blockchain-based decentralized security management.

5. **Measurement of Key Indicators**

   For both scenarios, the following metrics were measured:

   - Latency (end-to-end delay).

  - Identification and authentication time.
  - Resilience to attacks (e.g., controller overload, spoofing attempts).
  - Overall trust level among network components (trust index).

6. **Comparative Evaluation**

   Results from both scenarios were statistically compared to determine the impact of blockchain integration on performance and security.

2.3. Data Analysis

The collected data were analyzed using descriptive and inferential statistical methods. Specifically:

- Descriptive statistics were used to summarize latency, identification time, and trust index values.
- **t-tests** and **ANOVA** were applied to compare performance between the centralized and decentralized scenarios.
- Variance comparison methods were used to assess stability and resilience under different loads and attack conditions.

All performance indicators were evaluated with a **95% confidence interval**.

The simulation results demonstrated that the blockchain-integrated model operates more stably and efficiently than the traditional centralized SDN security approach. As a result of implementing blockchain-based smart contracts, the duration of the identification process:

- **decreased by 25–30% ($p < 0.05$)**,

thereby eliminating dependence on centralized certification servers and reducing the risk of bottlenecks.

The critical vulnerability associated with centralized SDN controller architectures—i.e., the single point of failure—was significantly mitigated due to the distributed nature of the blockchain.

Test results further showed that:

- **resistance to attacks increased by approximately 2.4 times**, and
- **overall system resilience improved**.

Based on measurements visualized in graphs and tables:

- blockchain integration generally kept system performance **stable**, and
- the increase in latency was **minimal (3–5 ms)**, remaining compatible with 5G quality-of-service requirements.

The evaluation of the **trust index** among network components indicated that:

- through the decentralized ledger, the **trust level increased by 20–25%**, and
- **data immutability was fully ensured**, strengthening auditability and non-repudiation.

3. Results and Discussion

The findings of the study indicate that integrating blockchain technology into 5G–SDN architectures significantly enhances the reliability and sustainability of security management. The **25–30% acceleration** in the identification process shows that security operations are better optimized in dense 5G environments with a large number of connected devices. This improvement reduces the load on traditional certification servers and facilitates near real-time security management.

These outcomes are consistent with theoretical models and frameworks proposed by Kumar and Singh (2022), Lin and Zhu (2024), and Al-Fuqaha et al. (2023), who argued that blockchain can improve trust and resilience in 5G–SDN systems. However, unlike many previous works, the present study demonstrates practical integration of blockchain into the SDN control plane under realistic simulation conditions, rather than remaining purely conceptual.

The main factors explaining why decentralized management improves security indicators include:

- the **immutability** of the distributed ledger, which prevents unauthorized modification of security logs;
- **automatic authorization** and policy enforcement through smart contracts;
- more **transparent and fine-grained monitoring** of threats and security events;
- the **distribution of control load** from a single centralized controller to a set of blockchain nodes and smart contract logic.

3.1. Limitations

Despite the positive outcomes, several limitations were encountered during the research:

- In certain configurations, **blockchain integration introduces minimal additional latency**, even if it remains within acceptable 5G bounds.
- The simulation environment, although realistic, **does not fully replicate a large-scale commercial 5G operator network**, where traffic volumes and heterogeneous services are far greater.
- The **security of smart contracts** themselves (e.g., against re-entrancy, logic bugs, or privilege escalation) was not exhaustively analyzed and requires separate, dedicated study.

3.2. Future Research Directions

In light of these limitations, future research is recommended in the following directions:

- **Integration of AI-based security agents** with blockchain mechanisms to detect anomalies and attacks more intelligently.

- **Development and evaluation of lightweight consensus algorithms** that further reduce latency and energy consumption for 5G-scale deployments.
- **Large-scale application tests in massive IoT environments**, where device numbers and heterogeneity pose unique challenges.

Overall, the research demonstrates that a blockchain-based decentralized management model can be an effective solution for optimizing security operations in 5G–SDN networks. The proposed model:

- automates identification and authentication processes,
- distributes trust without relying on a central authority,
- eliminates the **single point of failure** risk, and
- enables dynamic, programmable management of security policies through smart contracts.

This approach contributes significantly to reshaping the security architecture of future 5G, 6G, and massive IoT networks.

4. Proposed Blockchain-Based Decentralized Security Architecture

The proposed blockchain-based decentralized security model is designed to optimize security management processes in 5G–SDN networks and to minimize dependence on centralized structures in identification and authorization operations (Dorri et al., 2017). The architecture consists of **three functional layers**, each covering independent yet interconnected components of the network. Collectively, these layers support the processing of security events, traffic management, and the distributed storage of a trust ledger.

4.1. Network Management Layer

The **Network Management Layer** acts as the primary control tier responsible for decision-making and policy enforcement across the network. The SDN controller—serving as the central intelligent component of the SDN architecture—resides in this layer and coordinates security processes, including flow rule installation, traffic redirection, and interaction with the blockchain layer for authentication, authorization, and logging.

4.1. Network Management Layer

The **Network Management Layer** acts as the "brain" of the entire architecture, where high-level security and routing decisions are made. It hosts the SDN controller and coordinates both network operation and its interaction with the blockchain security layer.

Main functions include:

- **Policy management by the SDN controller.**

  Using platforms such as ONOS or OpenDaylight, the controller defines and installs flow rules, assigns priority levels, allocates resources, and configures security parameters across the network. In this way, quality of service (QoS), access control, and traffic isolation policies are centrally specified but later enforced in a distributed manner.

- **Integration with the blockchain interface.**

  The controller maintains a secure interface to the blockchain module via REST APIs, gRPC, or Web3.js–based SDKs. Through this interface, it sends smart contract calls (for example, to request authentication or update permissions) and receives responses that influence real-time security decisions.

- **Management of smart contract execution and auditing.** The controller orchestrates:
  - the **routing of identification requests** from user equipment (UE) or switches to the appropriate smart contracts,
  - **permission checking**, by querying smart contracts to verify whether a given node or flow is authorized, and
  - **logging of network events into the ledger**, ensuring that relevant security events (e.g., suspicious flows, access attempts) are immutably recorded.

- **Coordination of network security incidents.**

  When anomalies such as DDoS attacks, spoofing attempts, or unauthorized external access are detected, the controller generates appropriate mitigation policies (for instance, "deny rules" or rate-limiting rules) and immediately applies them in the data plane. This enables rapid reaction to emerging threats.

- **Load-balancing and fault tolerance with respect to blockchain nodes.** Based on the response time and availability of blockchain nodes, the controller distributes requests to the most suitable node or subset of nodes. This avoids overloading specific validators and supports high availability of the security-control path.

Overall, this layer provides a global, logically centralized view of the network, yet—thanks to blockchain integration—its decisions are anchored in a **decentralized trust infrastructure** rather than a single point of failure.

4.2. Data Layer

The **Data Layer** encompasses the physical and virtual components through which real traffic in the 5G network is transmitted and processed. It includes SDN switches, forwarding devices, and user equipment (UE). From a security point of view, this is the **most sensitive operational environment**, since all packets, flows, and real-time attacks manifest here. Blockchain-integrated identification and enforcement mechanisms are directly applied at this level.

Main functions include:

- **OpenFlow-based traffic forwarding.**

  Switches forward packets according to flow rules installed by the SDN controller. These rules determine the optimal path, priority, and treatment of each flow, ensuring efficient utilization of 5G network resources.

- **Packet identification and request forwarding.**

  When 5G user equipment (UE) first connects to the network, the initial identification request is forwarded—via the controller—to the relevant smart contract. Once the smart contract validates the identity and authorization, a corresponding "allow" flow rule is created and installed for that traffic. This process ties access control in the data plane directly to blockchain-backed verification.

- **Real-time defense against attacks.**

  The data layer is where real-time mitigation is enforced:

  - **Spoofing detection:** If identification hashes or credentials do not match those registered on the blockchain, the associated packets are automatically blocked at the switches.
  - **DDoS detection and mitigation:** Flow frequency, packet bursts, and anomalous behaviors are analyzed using tools such as sFlow and Wireshark, and compared with security event records stored on the blockchain. If suspicious patterns exceed thresholds, flows can be rate-limited or dropped.

- **QoS/QoE optimization for security operations.**

  To maintain 5G performance requirements, security functions are executed via a **"fast-path" mechanism**, where frequently used checks and policies are cached or pre-installed to minimize latency. This ensures that security enforcement does not significantly degrade user quality of experience (QoE).

In sum, the data layer is the **"operational field"** of the architecture: it is where security decisions, once made in the control and blockchain layers, are actually enforced on live traffic.

4.3. Blockchain Security Layer

The **Blockchain Security Layer** serves as the distributed trust and security backbone of the architecture. It provides the **trust, transparency, and immutability** properties that traditional centralized SDN controllers lack. By distributing verification and record-keeping across multiple nodes, it removes the single point of failure inherent in classical SDN control designs.

Main functions include:

- **Maintaining the distributed trust ledger.**

  The blockchain stores, in immutable blocks:

  - identification data of network nodes (e.g., UE, switches, controllers),
  - associated **permission levels** and roles,
  - **event logs** documenting access attempts, alerts, and incidents, and
  - relevant **network policies** related to authentication and authorization. This ledger functions as a shared, tamper-resistant memory of security-relevant state.

- **Smart contract–based security management.**

  Authentication, authorization, and security-event logging are handled automatically via smart contracts. These contracts encode rules for:

  - verifying identities,
  - granting or revoking permissions, and
  - recording anomalies or policy violations.

    Because these operations execute on-chain, they minimize human intervention and reduce the risk of administrative errors or insider threats.

- **Consensus algorithm for trust and consistency.**

  To maintain consistency among nodes, an appropriate consensus mechanism is selected based on system requirements:

  - **PBFT (Practical Byzantine Fault Tolerance):** provides high verification accuracy and strong fault tolerance, suitable for environments with strict correctness requirements.
  - **Raft:** emphasizes lower latency and faster decision-making, useful when responsiveness is critical.
  - **Proof-of-Authority (PoA):** offers fast block confirmation in **trusted operator environments**, where a limited set of known validators is acceptable.

- **Elimination of centralized vulnerabilities.**

  The blockchain layer directly addresses the **"single point of failure"** issue. Because each critical operation (e.g. identity registration, policy update) is confirmed by multiple nodes, the system becomes more resistant to attacks targeting individual controllers or servers.

- **Full transparency and auditability.**

  Every identification request, permission grant or revocation, and recorded security incident is written to the ledger in an immutable format. This ensures:

  - transparent post-incident analysis,

- strong non-repudiation, and
- the ability to reconstruct the complete history of security-related events.

In this sense, the blockchain security layer acts as the **"trust engine"** of the architecture. It manages security processes independently of any single centralized mechanism and provides a verifiable foundation upon which the SDN controller and data plane can safely operate.

Conclusion

Although the integration of 5G and SDN technologies plays a crucial role in shaping next-generation communication infrastructures, traditional centralized management models introduce serious security risks. The findings of this study show that, in classical SDN controller architectures, problems such as the single point of failure, dependence on centralized certification servers, delayed detection and mitigation of attacks, and the concentration of trust in a single control entity are not acceptable for highly dynamic and large-scale networks such as 5G. The proposed blockchain-based decentralized management model substantially mitigates these weaknesses.

Based on the simulation results, integrating the SDN control layer with the blockchain security layer accelerated identification and authentication processes by 25–30%, increased attack resistance by approximately 2.4 times, and raised the overall trust index by 20–25%. The immutability of the distributed ledger, automated authorization via smart contracts, and transparent auditing of security events together ensured the continuity, integrity, and reliability of network management. At the same time, the additional latency introduced by blockchain remained within the 3–5 ms range, which can be considered acceptable within standard 5G performance requirements.

The proposed three-layer architecture—Network Management Layer, Data Layer, and Blockchain Security Layer—clearly structures the functional distribution of security operations. Dynamic policy enforcement at the controller level, real-time defense mechanisms in the data layer, and the distributed trust ledger in the blockchain layer complement one another within a unified ecosystem. As a result, dependence of identification and authorization operations on centralized structures in 5G–SDN environments is reduced, and the overall process of making security decisions becomes more flexible, transparent, and resilient.

Several limitations of the study should be acknowledged. The simulation environment does not fully reflect deployment at real operator scale; blockchain integration can introduce additional latency in certain configurations; and smart contracts themselves require dedicated protection against sophisticated cyberattacks. Nevertheless, the obtained results confirm that a blockchain-based decentralized management model is a promising direction for redesigning the security architecture of 5G, 6G, and massive IoT networks.

Future research should focus on integrating AI-based security agents with blockchain, designing and testing more lightweight consensus algorithms, and implementing pilot deployments in real operator networks. These steps will further strengthen the practical potential of the proposed model and support the development of robust, trustworthy security ecosystems in next-generation communication infrastructures.

References

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2023). Secure and scalable 5G architectures using blockchain and SDN. Computer Networks, 225, 109545.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. 2017 IEEE PerCom Workshops, 1–6.

Kreutz, D., Ramos, F. M. V., Verissimo, P., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14–76.

Kumar, R., & Singh, P. (2022). Blockchain-enabled security framework for 5G-SDN networks. IEEE Communications Surveys & Tutorials, 24(3), 145–169.

Lin, X., & Zhu, Y. (2024). Decentralized trust management in 5G and beyond: A blockchain-based SDN approach. IEEE Transactions on Network and Service Management, 21(1), 58–74.

Zhang, Y., Yu, F. R., Zhang, M., Yao, J., & Liu, C. (2019). Blockchain-based distributed control and security architecture for 5G networks. IEEE Wireless Communications, 26(5), 24–31.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper.