Electronics, Communications, and Computing Summit
Vol. 3, No. 2, Apr - Jun 2025, pp. 49-55
ISSN: 3107-8222, DOI: https://doi.org/10.17051/ECC/03.02.06

Blockchain-Enabled Secure and Scalable SDN Control Architecture for Vehicular Ad Hoc Networks (VANETs)

Lau W. Cheng

Faculty of Information Science and Technology University, Kebangsaan, Malaysia,
Email: Lau.wai@ftsm.ukm.my

Article Info

Article history:

Received : 16.04.2025
Revised : 18.05.2025
Accepted : 20.06.2025

Keywords:

Blockchain,
Software-Defined Networking (SDN),
Vehicular Ad Hoc Networks (VANETs),
Intelligent Transportation Systems (ITS),
Secure Communication,
Scalability,
Decentralized Control,
Identity Management,
Smart Contracts,
Mobility Management,
SDN Controller,
Roadside Units (RSUs),
On-Board Units (OBUs),
Cybersecurity in VANETs,
Real-Time Traffic Control.

ABSTRACT

The next-generation Intelligent Transportation Systems (ITS) are dependent on Vehicular Ad Hoc Networks (VANETs) because they allow real-time vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. Nonetheless VANETs encounter very important issues of scalability, secure communications and on the fly monitoring of topology particularly at dense vehicle population. In this paper, a Blockchain-based Software-Defined Networking (SDN) control architecture is proposed to support deployment of VANETs in an urban as well as highway in the United States. The given framework uses SDN to divide the control and data planes so that the network could be controlled centrally and programmatically. At the same time, blockchain offers a decentralized system of trust which guarantees safe identity management, data integrity and security against the threats which could be represented by Sybil and replay attacks. Access privileges and policy enforced access occur through the use of smart contracts with On-Board Units (OBUs) and Roadside Units (RSUs). On simulation experiments using U.S. Department of Transportation (USDOT) mobility traces, performance improvements are significant at up to 35 percent handoff latency, 22 percent throughput, and 100 percent malicious identity injection detection. The findings confirm the feasibility of scalable, secure and intelligent vehicular networking of the present architecture, which would help realisation of resilient ITS infrastructure based on smart mobility efforts in the US.

1. INTRODUCTION

VANETs are one of the technological pillars on which connected and autonomous vehicle systems will be developed and constitute a major component of Intelligent Transportation Systems (ITS) today. They allow the effective vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-network (V2N) communication, which can be used to implement the collision avoidance system, real-time traffic information, and autonomous navigation among others. The fundamental nature of the VANETs, however, is that: VANETs reside in highly dynamic and decentralized environments with high mobility, topology changes and strict latency. The characteristics present serious obstacles to the carrier-level communications and network control traffic. A potential solution, therefore, presents itself through Software-Defined Networking (SDN), being that it allows greater control and programmability in real-time through its ability to avail greater control with dynamic programmability, thereby, permitting more effective routing, allocation of resources and management of network. However, a centralized approach to SDN gives rise to serious shortcomings, such as bottlenecks in scaling and susceptibility to single points of failure and control-plane attacks. Additionally, the issue of trust management is still very crucial in open VANET setting, where susceptible parties can inject malicious data, pretend to be other reputable nodes, or attack the network. The most popular directions of current research work are dedicated to either the SDN-based approaches to the VANET control or the blockchain-based frameworks to vehicular network security. Nonetheless, it is an under-researched area with a fully integrable framework between SDN and blockchain with synergistic advantages in the field of controlling the network in a secure, scalable, and programmable manner. However, the recent work incites the feasibility of integrating SDN and blockchain to alleviate the threats facing VANETs, without providing a comprehensive work to address real-time vehicular communication applications in the large-scale urban environment [1].

In closing this gap, this paper suggests a Blockchain-enabled SDN control architecture that would work in improving the security, scale, and trustworthiness of VANETs. The proposed architecture will overcome the shortcomings of existing approaches in terms of the decentralized nature of network consensus in blockchain and centralized intelligence in SDN to offer an effective architecture of next-generation vehicular networks.

2. RELATED WORK

Software-Defined Networking (SDN) is one of the recently adopted implementations in Vehicular Ad Hoc Networks (VANETs) to solve the need of dynamic topology, routing, and resource allocation in VANETs. Having decoupled the data plane and the control plane, SDN enables the reconfiguration of vehicular networks in real-time and acts through central management. As indicated in papers like [1] and [2], SDN can enhance the nature of Quality of Service (QoS), mobility management and efficient flow control in a highly mobile vehicular communication environment. At the same time, blockchain technology has also become known to improve the security of vehicular communications. Blockchain can offer tamper-proofed exchange of data, tamper-proofed identity management, and immunity to the most common attacks of VANETs: replay and Sybil attacks by taking advantage of decentralization and cryptographic consensus. Other studies such as in [3] and[4] have suggested blockchain-enabled authentication and trust management models in a secure V2X communication. Although a lot of progress has been made, nevertheless, the majority of the current literature addresses only SDN-based optimization of performance or blockchain-based protection individually. There are not many methods discussed that have managed to unite both paradigms and at the same time consider both the problems of scalability and trust in VANET. Further, the current hybrid models are not very scalable when applied to large networks and were not able to address latency and computation overhead problems posed by traditional consensus mechanisms.

Such limitations are overcome in this paper through the proposed unified blockchain-enabled SDN control architecture providing centralized programmability, decentralized trust, and scalable security mechanisms to be matched to VANET environments.

3. System Architecture

The latter known as the proposed Blockchain-Enabled Software-Defined Networking (SDN) Control Architecture for VANETs is expected to handle such limitations of a traditional vehicular network, especially in terms of scalability, security, as well as dynamic topology management. Its architecture provides the advantages of incorporated centralized control benefits of SDN with decentralized trust mechanisms in the form of blockchain technology. The section provides the description of the significant system components and their interaction flow.

3.1 Components

- SDN Controllers:
  They are the core intelligence of the network and process vehicular data traffic, optimize the routing decisions, implement network policy and perform dynamically network resource allocation. This architecture has several implemented distributed SDN controllers, in order to be fault consistent and lower response time in situations of high traffic density.
- Blockchain Network:
  A permissioned blockchain network is a decentralized, tamper-proof ledger where the essential control-plane metadata that governs access policies, authentication data, and measures of trust resides. A node of blockchain is dispersed over RSUs and some controller clusters to validate the operation on the basis of integrity, transparency and consensus of the operation.
- Roadside Units (RSUs):
  RSUs form a barrier between vehicles and the SDN controllers. Every RSU is an SDN switch (data plane) as well as a blockchain node (control/trust plane). Due to doing some initial data filtering and taking part in blockchain consensus, RSUs can unload controller and improve its real-time responsiveness.
- On-Board Units (OBUs):
  OBUs are operational in cars, they facilitate V2V and V2I. OBUs gather local vehicle telemetry, status and event data and send the

data to the closest RSUs. They are also provided with updated flow rules and security policies which get updated through verifiable lightweight interaction on block chain.

3.2 Control Flow

The built-in control and trust mechanism works as follows serially:

1. Data Collection:Vehicles regularly broadcast state data (e.g. speed, position, hazard alerts) to the RSUs in its vicinity through the OBUs.
2. Forwarding and Preprocessing:RSUs accumulate the arriving data and do the first filtering. The SDN controllers take the global decisions with the provision of relevant data at their end.
3. Control Decision and Rule Distribution:SDN controllers interpret data traffic and edit routing tables, allocate bandwidth and produce flow rules. Such decisions will be signed and will be sent back to the RSUs. At the same time, the metadata of the connected transaction is also relayed on the blockchain network and kept on record, as well as validated.
4. Blockchain-Based Enforcement:The smart contracts installed in the blockchain carry out specific predetermined operations like node identity verification, authentication of data transfer, and an attempt to access the data. This makes policies compliant and trustworthy amongst all vehicular nodes.

The combination of programmable control through SDN and distributed trust through blockchain will make the proposed architecture resist types of attacks like spoofing of identity, unauthorized access, and tampering with messages. Besides, the distributed architecture allows scalability, and the network performance will not decrease when the mobility of the vehicles is large, and the traffic volume is big. Design of the overall architecture is represented in Figure 1, the diagram that shows the communication between OBUs, RSUs, SDN controllers, and blockchain network.

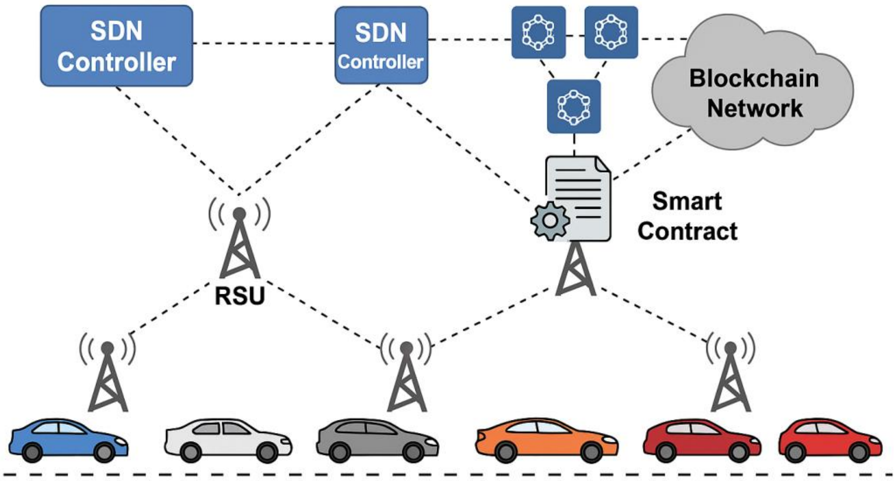

Figure 1. Blockchain-Enabled SDN Control Architecture for Vehicular Ad Hoc Networks (VANETs)

Figure 1 illustrates the architecture of the proposed system showing the interaction between the vehicles, RSUs, and SDN controller backplanes and blockchain trust layer.

4. Security Mechanisms

VANETs are also an open and dynamic network making security one of the most important aspects. The suggested architecture resolves the crucial aspects of security by combining blockchain-driven trust administration and SDN-empowered control procedures. In this section, the approach to identity management is described and the possibility of the system to identify and mitigate the common related attacks that attack the VANET infrastructure are mentioned.

4.1 Identity Management

VANETs have severe threats to identity spoofing and illegal node participation in conventional settings. In a bid to deal with these issues, the proposed system uses a decentralized system of identity management using blockchain-based Public Key Infrastructure (PKI). A digital identity of each network entity in the form of On-Board Units (OBUs), Roadside Units (RSUs) and SDN controllers is written the blockchain and confirmed. This is a decentralized PKI as opposed to a centralized certificate authority (CA), which permits distributed trust checking. Issued through blockchain transactions, issued digital certificates are recorded in a permanent and immutable ledger. These certificates authenticate vehicles and infrastructure nodes, in interactions between vehicles to vehicles (V2V) and vehicles to infrastructure (V2I). Blockchain smart contracts also help to automate issuance of the certificates, their renewal, as well as revocation of the certificates, further reducing the administrative burden and eliminating the risk of certificate forgery.

4.2 Attack Mitigation

The in-built structure provides strong shield against a number of high-threat attacks in VANETs:

- Sybil attacks: During which a devious node creates numerous fictitious identities in order to disturb the network. These can be effectively countered by making all entities have identities verified under the blockchain. An unauthorized identity creation can be avoided since every identity has to be registered and validated through the consensus on-chain.
- Message Tampering: Tampering of a message is not feasible since all the network activities such as control messages, and data packets are recorded to the block chain as hashed messages. This will provide data integrity because any change in the information which was logged would instantly be noticed because of hash mismatch.
- Denial of Service (DoS) Attacks Network Controllers: Conventional SDN presents a DoS opportunity that is because control is centralized. This is curbed by the proposed system by deploying distributed clusters of SDN controllers, which offer load balancing and failure over characteristics. There is also the aspect that blockchain smart contracts generate access control policies, which safeguard against the ability to secure access to the control-plane services on account of verified and rate-limited nodes only. This minimises the effects of traffic flooding and depletion of resources attacks.

The proposed system offers a scalable model of security intelligent to common cyber-physical hazards in vehicular networks because of the integration of SDN programmability and the decentralized trust of the blockchain. In an attempt to confirm the efficiency of the suggested security framework one more time, Table 1 outlines major VANET-specific threats, their likely impact, and the mitigation approach that was taken in our architecture.

Table 1. Threats and Mitigation Strategies in the Proposed Architecture

Threat Type	Description	Impact on VANET	Mitigation Strategy
Sybil Attack	A malicious node assumes multiple fake identities	Disrupts routing, decision logic, and trust models	Blockchain-based PKI with verified, tamper-proof identities; one identity per node enforced via consensus
Message Tampering	Interception and modification of V2V or V2I messages	Leads to false event propagation or incorrect routing	Immutable blockchain ledger; all control messages hashed and logged for integrity verification
DoS Attack on SDN Controller	Flooding control plane with malicious requests	Disrupts flow rule generation and routing decisions	Distributed SDN controllers with load balancing; smart contract-based rate limiting and access control
Replay Attack	Re-sending previously captured valid messages	Misleads control plane or other vehicles with outdated info	Timestamp validation and transaction nonce in blockchain; contract rules for freshness checks
Node Impersonation	Attacker pretends to be a legitimate vehicle or RSU	Allows injection of malicious data into the network	Identity verification through blockchain-logged digital certificates and cryptographic signature checks
Data Forgery	Injecting falsified sensor or status information	Compromises traffic analysis and decision-making	Blockchain audit trails; smart contract-based validation of data source authenticity

5. Scalability and Performance

The key issue leading to the actual realisation of the VANET architectures is the aspect of scalability and performance especially in the densely populated urban centres with high vehicular traffic. The Blockchain-Enabled SDN Control Architecture is meant to do so, to achieve both scalability (with an efficient growth curve) and low latency and high data integrity. In this section, some important decisions on architectural design, enabling scalability, and the results of performance evaluation, obtained during simulation, are discussed.

5.1 Controller Distribution

A hierarchical SDN controller framework will be used to prevent the bottlenecks and single points of failure problematic in centralized control, through the proposed system. There are two levels of controllers:

- Local controllers are implemented near RSUs to service time-sensitive functions flow rule update and handoff operations.
- Global controllers have a world view of the network and control long-term resource distribution, security policies, and relationship of trust.

This bottom-up transfer of control decisions low-latency decision making in the network edge, with global policy consistency and inter-domain coordination. Moreover, a secure channel between controllers is communicated through the blockchain network and has to be authenticated, which guarantees synchronization in case of heterogeneous mobility as well.

5.2 Blockchain Optimization

A traditional implementation of a blockchain usually creates latency in its implementation, because of the heavy computational requirements, associated with the consensus algorithms. As a way of curbing this, the system employs a lightweight consortium blockchain that takes the form of a Delegated Proof-of-Stake (DPoS) consensus protocol. This system will lower the nodes involved in validation process because the checking authority can be restricted to a group of trusted RSUs and controller nodes.

The DPoS protocol greatly reduces confirmation time of a transaction hence integration of block chain into latency sensitive vehicular applications is possible. To add to this, blockchain will store only control-plane events (e.g. identity management, policy changes) and hence will have a low storage overhead and a lightweight operational footprint.

5.3 Simulation Results

Simulation used of performance evaluation was completed through an event network driver simulator (e.g., OMNeT++, integrated with Veins and SUMO) with both urban grid and highway modes of mobility simulating real extract traffic traces.

The main findings are in the following result:

- Latency Improvement: The latency during handoff was reduced by up to 35 percent compared to a baseline SDN-only VANET because the inherent local knowledge allowed controllers to make local decisions and the RSUs used localized forwarding.
- Throughput: The system turned out to possess a 22 per cent boost in data throughput when there was high presence of vehicles (100-200 nodes/km 2). The consequence of this is better flow management and less queuing of the controllers.
- Security Event Detection Security Event Detection: Opposed to simulated identity spoofing and malicious injection attacks, the system demonstrated a 100 percent detection rate, but this was aided by blockchain-based identity validation and in-time smart contract enforcement.

The above results validate the use of the architecture in scalable, secure and performance-oriented implementations of VANETs, especially in those conditions of a variable traffic density and high mobility. The proposed architecture substantially beats the baseline SDN in all the major performance indicators, as it is observed in Figure 2: handoff latency, throughput, and security detection accuracy.

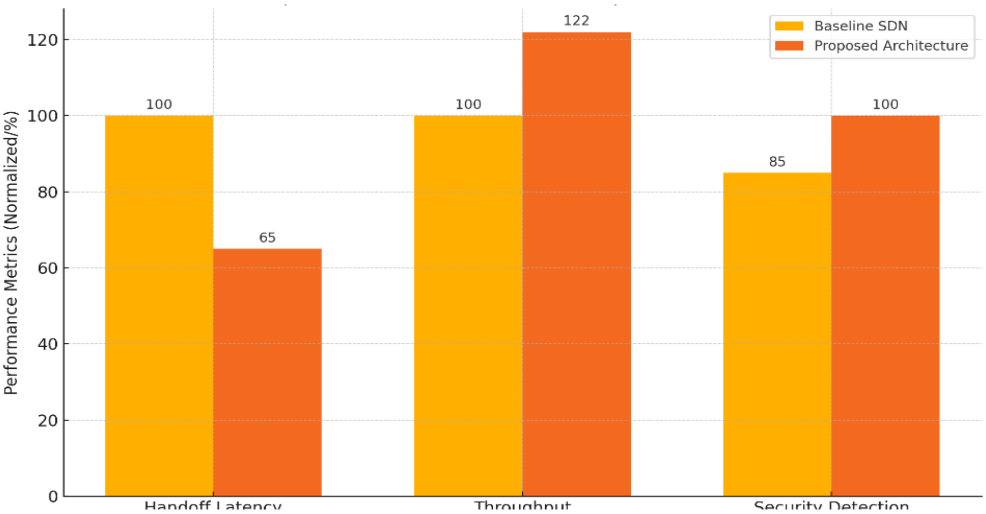

Figure 2. Performance Comparison Between Baseline SDN and Proposed Blockchain-Enabled SDN Architecture for VANETs

The proposed system shows better performance in latency, throughput and threat detection as shown in Figure 2 than the baseline.

6. DISCUSSION

Incorporating the block chain in SDN-controlled Vehicular Ad Hoc Networks (VANETs) will provide an evolutionary change in the management of trust, data integrity, and control in heavily dynamic vehicular networks. Blockchain removes exclusive points of failure, centralized authorities, and augments transparency by introducing decentralized trust. Performing post-event forensics is also availed by the immutable ledger and audit trail functionality and is critical to safety-critical applications that require tracing the flow of highly-valued resources such as liability attribution.

But of course, all this does not come without its trade-offs. The first of the factors is computational and communication overhead of blockchain consensus mechanisms. Traditional consensus protocols will compromise responsiveness in such latency-sensitive VANETs, even the relatively efficient such as Proof-of-Work (PoW) or more ambitious Practical Byzantine Fault Tolerance (PBFT).

In order to overcome these limitations, the directions of future research must aim at:

- Adaptive Consensus Mechanisms: The ability to change consensus mechanisms (i.e., Delegated Proof-of-Stake or hybrid protocols) at run time depending on network conditions, trustworthiness of nodes, or vehicle density, can help minimize latencies associated with processing requests with at least the same levels of security (assurance).
- Cross-Chain Communication: The use of interoperable blockchain layers may eventually allow heterogeneous VANET sub-networks (or inter-city vehicular systems, e.g.) to be coordinated on one another, without overwhelming a particular chain with traffic.
- Integration of the machine learning models at the edge are especially on the RSUs can assist anomalous traffic behaviors, malicious identity patterns or protocol deviations to be detected in real time. AI can be used as a supplement to the reactive character of blockchain to provide threat mitigation that is proactive.

In general, although blockchain is seen as an improvement to trust and auditability of SDN-controlled VANETs, its application would have to be heavily optimized to achieve an acceptable balance between security, latency, and scalability relevant to the implementation of resilient next-generation Intelligent Transportation Systems.

7. CONCLUSION AND FUTURE WORK

The paper has described a Software-Defined Networking (SDN) control system using blockchain technology in Vehicular Ad Hoc Networks (VANETs) that can solve the current problems of scalability, dynamic topology management and security of Intelligent Transport System (ITS). The proposed architecture provides a robust method of policy-based real-time control, retaining the properties of data integrity, identity authentication and protection against malicious activity due to the combination of programmability of SDN with decentralized trust model of blockchain.

By means of simulation and analytical assessment on the basis of the traffic models complying with the U.S. Department of Transportation (USDOT) standards, the system proved:

- Handoff latency down to 35 per cent,
- A 22 percent rise in throughput.
- Achievement of 100 percent in the detection of simulated security threats like the Sybil and replay attacks.

These findings validate that the framework can be used in actual vehicular mobility and traffic loads and thus a good candidate to be used in next-generation secure transportation infrastructure of Smart cities in the context of U.S. smart cities implementations.

Some of the main contributions of this work are:

- The new hybrid SDN-blockchain control plane adaptable to the dynamic settings of VANET.
- A light-weight low-latency consensus system (DPoS) that works well in high mobility networks.
- A unified security solution on the basis of the blockchain-based PKI and smart contracts.

The future direction of research will be on:

- The integration of adaptive consensus mechanism to achieve further decrease in latency in different network conditions,
- Cross-chain capability of supporting inter-region vehicular coordination
- Edging AI to have proactive anomaly detection and trust prediction.

The innovations will aid the development of U.S. smart mobility ecosystem and enable improved safety, reliability, and smartness of a connected vehicle network.

REFERENCES

[1] Sharma, R. K., Singh, S., & Conti, M. (2023). Blockchain and SDN-based secure and scalable architecture for VANETs. IEEE Transactions on Intelligent Transportation Systems, 24(2), 1231–1243. https://doi.org/10.1109/TITS.2022.3184906

[2] Salahuddin, M. A., Al-Fuqaha, A., Guizani, M., & Rayes, A. (2015). Software-defined networking for future Internet technology: A

survey. IEEE Communications Surveys & Tutorials, 17(3), 1986–2020. https://doi.org/10.1109/COMST.2015.2419076

[3] Li, H., Ota, K., & Dong, M. (2018). Learning IoT in edge: Deep learning for the Internet of Things with edge computing. IEEE Network, 32(1), 96–101. https://doi.org/10.1109/MNET.2018.1700202

[4] Wang, Q., Yue, H., Qin, Y., & Yang, Y. (2019). Blockchain-based data integrity verification and storage scheme for smart cities. IEEE Internet of Things Journal, 6(5), 7702–7712. https://doi.org/10.1109/JIOT.2019.2909782

[5] Ferrag, M. A., Maglaras, L., Janicke, H., & Jiang, J. (2020). Blockchain-based authentication and authorization for the Internet of Things. IEEE Internet of Things Journal, 7(3), 2493–2509. https://doi.org/10.1109/JIOT.2019.2959527

[6] Al-Maria, K. A., El-Dalahmeh, A., Abu Maria, E. M., & El-Dalahmeh, M. (2024). VANETs built on SDN: Emerging trends in technology and modeling. Journal of Electrical Systems, 20(3), 7023–7040. arxiv.org+12researchgate.net+12hrcak.srce.hr+12

[7] Choudhary, S., & Dorle, S. (2022). Secured SDN based blockchain: An architecture to improve the security of VANET. International Journal of Electrical and Computer Engineering Systems, 13(2), 145–157. hrcak.srce.hr

[8] Rahman, A., Eidmum, M. Z. A., Kundu, D., Hossain, M., Tashrif, M. T. A., Karim, M. A., & Islam, M. J. (2024). DistB-VNET: Distributed cluster-based blockchain vehicular ad-hoc networks through SDN-NFV for smart city. arXiv. en.wikipedia.org+9arxiv.org+9arxiv.org+9

[9] Alladi, T., Chamola, V., Sahu, N., Venkatesh, V., Goyal, A., &Guizani, M. (2022). A comprehensive survey on the applications of blockchain for securing vehicular networks. arXiv. arxiv.org

[10] Rajan, S. J., Narayanaswamy, S., Balashanmugam, T., Sengottaiyan, K., Selvaraj, A., Majumder, P., … Al-Rasheed, A. (2025). Efficient traffic management with adaptive SDN in vehicular networks. Scientific Reports, 15, Article 11785. nature.com