Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

An Identity-Aware Permissioned Blockchain Architecture for Secure Connected Vehicle Communication

Md Shahanur Islam Shagor

smshagor.ru@gmail.com

Voronezh State University of Forestry and Technologies https://orcid.org/0009-0003-7730-3202

Research Article

Keywords: Blockchain, connected vehicles, identity authentication, Internet of Vehicles, permissioned blockchain, replay protection, V2X security, Byzantine fault tolerance

Posted Date: September 18th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11073229/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

An Identity-Aware Permissioned Blockchain Architecture for Secure Connected Vehicle Communication

Md Shahanur Islam Shagor

Independent Researcher, Department of Computer Science and Microelectronics Engineering,
Voronezh State University of Forestry and Technologies, Voronezh, Russia

Corresponding author: smshagor.dev@gmail.com

ABSTRACT—Connected vehicles exchange safety-critical messages over communication channels that are exposed to identity spoofing, replay, equivocation, and infrastructure compromise. This paper presents an identity-aware permissioned blockchain architecture that binds vehicular message admission to authenticated identities while preserving low-latency message dissemination. The design separates real-time message propagation from ledger ordering: vehicles sign canonical V2X messages using short-lived pseudonymous credentials; roadside gateways perform first-stage verification and freshness screening; and a permissioned Byzantine-fault-tolerant validator set records compact authenticated event commitments. Sequence numbers, epochs, nonces, parent-block linkage, validator certificates, and deterministic fork-choice rules jointly provide replay resistance and ledger consistency. A formal threat model considers forged identities, duplicated messages, compromised validators, double signing, stale blocks, and temporary network partitions. Security arguments show that an attacker without a valid signing key cannot create an admissible vehicle event, while safety is maintained when fewer than one third of validators are Byzantine under the stated quorum model. A controlled discrete-event simulation evaluates 10–500 active vehicles and adversarial validator ratios up to 40%. The proposed architecture sustains 1,910 authenticated events/s at 100 vehicles with 66 ms median end-to-end finality, and it retains a 99.2% invalid-event rejection rate at 30% malicious validators. Compared with a conventional PBFT deployment, the architecture reduces finality latency by 52.5% and increases throughput by 94.9% at 100 vehicles by moving duplicate filtering and identity validation ahead of consensus. The results indicate that identity-aware admission and permissioned ordering can provide a practical security-performance balance for auditable connected-vehicle communication without placing the full safety-message stream on-chain.

INDEX TERMS—Blockchain, connected vehicles, identity authentication, Internet of Vehicles, permissioned blockchain, replay protection, V2X security, Byzantine fault tolerance.

I. INTRODUCTION

Vehicle-to-everything (V2X) communication has become an important component of cooperative driving, traffic coordination, fleet supervision, and road-safety applications. A connected vehicle can exchange position, speed, maneuver intent, hazard notifications, and infrastructure status with neighboring vehicles and roadside equipment. The value of these messages depends on two properties that are difficult to maintain simultaneously: the information must arrive within a safety-relevant delay bound, and the receiver must be able to determine whether the sender and the message are authentic. Standards such as IEEE 1609.2 therefore place strong emphasis on authenticated messages and credential management, yet the operational environment remains challenging because vehicles join and leave communication domains rapidly and infrastructure components may be administered by different organizations [1].

Conventional public-key infrastructures provide an effective basis for message signing, but they do not by themselves provide a shared, tamper-evident view of enrollment, revocation, validator decisions, or conflicting security events across administrative boundaries. Centralized security back ends can maintain such state, although they introduce a high-value point of failure and make independent audit difficult. Blockchain systems address the latter concern by replicating an ordered record across multiple parties, but directly placing all V2X traffic on a blockchain is inappropriate for latency-sensitive communication. Public-chain consensus introduces unnecessary delay and cost, while naive permissioned designs can still suffer from excessive validator communication, replayed transactions, and identity ambiguity.

Prior work has explored blockchain-assisted authentication, key management, access control, anonymous credential management, and secure V2V communication [2]–[8]. These studies establish that distributed ledgers can support vehicular trust functions, but three design gaps remain important for operational deployment. First, identity validation is frequently treated as a separate authentication step rather than as a mandatory ledger-admission condition. Second, freshness protection is often defined for the network message but not consistently propagated into the consensus object, leaving ambiguity about duplicated or reordered security events. Third, performance evaluations commonly measure authentication cost or blockchain throughput in isolation, although the critical quantity for a connected-vehicle security plane is the combined delay from signed-message generation to auditable finality.

This paper develops an identity-aware permissioned blockchain architecture designed around these gaps. The central design principle is that safety messages continue to propagate through the low-latency V2X path, while only compact authenticated event records are submitted to the ledger. A vehicle message is accepted for ledger ordering only after its pseudonymous credential, digital signature, epoch, monotonic sequence number, and nonce have been verified. Validators therefore do not spend consensus bandwidth on obviously invalid or duplicate events. The consensus layer uses a Byzantine quorum certificate and parent-linked blocks so that finalized events have deterministic ordering and equivocation evidence can be retained for audit.

The main contributions are fourfold. First, an identity-aware admission model binds each ledger event to a validated vehicular credential without exposing a long-term identity in routine messages. Second, a layered anti-replay construction combines epoch-scoped sequence numbers, nonces, a replay cache, and ledger-level uniqueness. Third, a permissioned quorum protocol integrates fork rejection, validator double-sign detection, and deterministic finality. Fourth, a controlled simulation evaluates the integrated data path over 10–500 active vehicles and adversarial validator ratios up to 40%, reporting finality latency, throughput, communication load, and invalid-event rejection. Unlike designs that make the blockchain the transport substrate, the proposed architecture treats the ledger as an auditable security control plane.

II. RELATED WORK AND RESEARCH GAP

A. Blockchain-Assisted Vehicular Authentication

Blockchain-assisted vehicular security has developed along several complementary lines. Lu et al. proposed blockchain-supported authentication and key management for vehicular ad hoc networks, combining edge infrastructure with a consortium ledger to support group

membership and key updates [2]. Das et al. later presented a blockchain-enabled V2V system in which smart contracts participate in user and vehicle authentication and unauthorized-access detection [3]. These designs demonstrate the utility of a replicated authorization record, but they primarily focus on authentication workflows rather than the joint treatment of identity, message freshness, and consensus-object uniqueness.

Su et al. combined consortium and private blockchains with privacy-preserving authentication, short signatures, homomorphic encryption, and pre-authentication to reduce handover cost [4]. Liu et al. proposed consortium-chain credential management for anonymous authentication in integrated vehicular networks, showing how distributed setup and succinct commitments can improve credential verifiability [5]. More recently, Li et al. investigated revocable cross-domain authentication using blockchain-supported distributed trust across heterogeneous domains [6]. These approaches improve privacy and cross-domain operation; however, their primary objective is credential or authentication efficiency rather than a complete event-admission path with explicit replay and fork controls.

B. Secure Communication, Access Control, and Privacy

Hussain et al. proposed a blockchain-enabled secure communication framework for the Internet of Vehicles that emphasizes trust and access control [7]. Jiang and Lv used a blockchain with zero-knowledge-based authentication and distributed storage to improve privacy and scalability [8]. Chen et al. proposed a lightweight blockchain-enabled authentication protocol for transportation cyber-physical systems and analyzed resistance to several attack classes [9]. Collectively, these studies show that blockchains can strengthen identity management and authorization, but they also illustrate an architectural tension: cryptographic processing and ledger interaction must not delay safety-critical V2X dissemination.

This work therefore separates message transport from auditable ordering. It is not intended to replace IEEE 1609.2 message security or application-specific safety logic. Instead, it defines a permissioned control plane in which validated identities, event digests, revocation decisions, and consensus evidence can be shared among trusted infrastructure operators. The distinction is important because it allows the security properties of distributed ordering to be used without requiring every neighboring vehicle to participate in blockchain consensus.

TABLE I Positioning of the proposed architecture relative to representative vehicular blockchain approaches.

Approach	Primary focus	Identity-bound admission	Replay-aware ledger event	Byzantine fork control
Lu et al. [2]	Auth. + key management	Partial	No explicit ledger binding	Consortium dependent
Das et al. [3]	V2V smart-contract security	Yes	Limited	Not central
Su et al. [4]	Privacy-preserving auth.	Yes	Message-level	Hybrid-chain dependent
Liu et al. [5]	Anonymous credentials	Yes	Not primary	Consortium dependent
Proposed	Identity + freshness + ordering	Yes	Yes	Explicit quorum + parent linkage

III. SYSTEM MODEL, THREAT MODEL, AND DESIGN OBJECTIVES

A. Network and Trust Model

The system contains vehicles V={v1,...,vn}, roadside or edge gateways R={r1,...,rk}, and permissioned validators P={p1,...,pm}. Vehicles are not validators by default. Each vehicle contains an on-board unit capable of signing V2X messages with a short-lived pseudonymous private key. A credential authority issues a pseudonymous credential that binds the corresponding public key to an authorized vehicle enrollment while retaining the long-term registration mapping outside routine communication. Roadside gateways maintain the current credential-status material and forward only admissible event records to validators.

Validators are operated by authorized transportation, fleet, infrastructure, or service stakeholders. The consensus assumption is m >= 3f+1, where at most f validators are Byzantine during a consensus instance. Network delivery may be delayed or temporarily partitioned, but messages between honest validators are eventually delivered after the network becomes synchronous. These assumptions are consistent with permissioned Byzantine-fault-tolerant operation; they do not claim safety against a majority takeover.

TABLE II Principal notation.

Symbol	Meaning
V, R, P	Vehicle, roadside gateway, and validator sets
IDp	Short-lived pseudonymous vehicle identifier
pkv, skv	Vehicle verification/signing key pair
e, s, n	Epoch, monotonic sequence number, and random nonce
H(.)	Collision-resistant cryptographic hash
σv	Vehicle signature over the canonical message
QC	Validator quorum certificate
f	Maximum Byzantine validators tolerated
Δfresh	Maximum accepted message-age window

B. Message and Event Model

A vehicle constructs a canonical safety or telemetry message M from its pseudonymous identifier, application type, timestamp, epoch, sequence number, nonce, payload digest, and optional context. The canonical byte representation prevents semantically equivalent messages from producing different signatures because of serialization ambiguity. The signed message is

$$M = IDp \,||\, type \,||\, t \,||\, e \,||\, s \,||\, n \,||\, H(payload) \,||\, context \quad (1)$$

$$\sigma v = Sign(skv, H(M)) \quad (2)$$

The roadside gateway verifies the credential status and signature before constructing a compact ledger event E. The event includes H(M), the credential identifier, freshness fields, gateway decision, and the message class; the full payload need not be stored on-chain. This separation reduces storage growth and avoids turning the blockchain into a broadcast channel for high-rate safety data.

$$E = H(M) \,||\, IDp \,||\, e \,||\, s \,||\, n \,||\, decision \,||\, type \quad (3)$$

C. Threat Model

The adversary can eavesdrop on wireless channels, replay previously valid signed messages, inject unsigned or malformed traffic, compromise a subset of vehicles, and control up to f validators. A Byzantine validator may refuse to vote, double vote, attempt to extend a stale parent, or propose a block containing duplicated events. The adversary may also exploit temporary network partitions to create competing proposals. Cryptographic hash functions and digital signatures are assumed secure. Compromise of the credential authority or more than f validators is outside the primary fault model and is discussed as a limitation.

TABLE III Threats and corresponding controls.

Threat	Control
Identity spoofing	Credential validation + vehicle signature
Wireless replay	Epoch/sequence/nonce freshness gate
Duplicate ledger submission	Event-key uniqueness + replay cache
Validator double vote	Signed vote evidence + slashing/administrative action
Stale/forked block	Parent-hash check + quorum certificate

Malformed event flooding	Gateway pre-validation + rate limiting
Temporary partition	No conflicting finality under quorum intersection; liveness resumes after synchrony

IV. PROPOSED IDENTITY-AWARE PERMISSIONED BLOCKCHAIN

A. Layered Architecture

The architecture is divided into three planes. The communication plane carries ordinary V2V and V2I messages and preserves the timing behavior expected by safety applications. The admission plane, implemented at trusted roadside or edge gateways, validates credentials, signatures, message format, freshness, and local policy. The consensus plane receives only compact admissible events and provides replicated ordering, finality, and audit evidence. This layered arrangement is shown in Fig. 1.

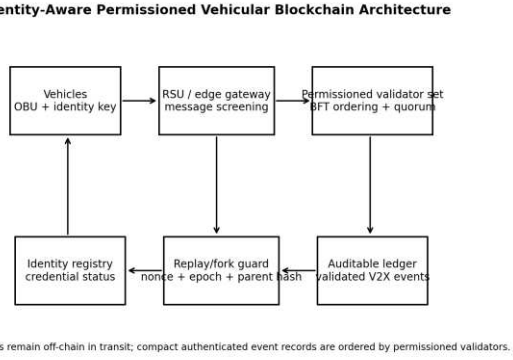


FIGURE 1. Identity-aware permissioned vehicular blockchain architecture.

B. Identity Lifecycle and Pseudonymous Admission

Long-term vehicle identities should not be broadcast with every V2X message. Enrollment therefore produces a set of short-lived pseudonymous credentials. A credential contains a pseudonymous identifier IDp, public key pkv, validity interval, issuer identifier, and authorization profile. Gateways verify the issuer signature and check revocation state before accepting a message. Because the blockchain event stores the credential identifier and message digest rather than a long-term identity, routine auditing can determine whether a valid enrolled credential produced an event without exposing the persistent civil or account identity of the vehicle.

Credential rotation is handled by epoch transitions. When a vehicle activates a new pseudonymous credential, its per-credential sequence state starts from a defined initial value and the previous credential is not reused beyond its validity interval. A revocation event invalidates subsequent messages from the affected credential after the revocation becomes effective. This design does not claim unlinkability against a global traffic-analysis adversary; its objective is operational pseudonymity while preserving accountable enrollment.

C. Multi-Layer Replay Resistance

A single timestamp check is insufficient in high-mobility networks because clocks can drift and an attacker may replay a message within the permitted skew interval. The architecture therefore defines an event key K_E from the pseudonymous identity, epoch, sequence number, and nonce:

$$K_E = H(IDp \,||\, e \,||\, s \,||\, n) \quad (4)$$

A gateway accepts a message only when four conditions hold: the credential is valid, the signature verifies, $|t_now - t| <= \Delta fresh$, and the tuple (e,s,n) has not been accepted previously for the same credential. Gateways retain a bounded replay cache for the active epoch. Validators perform a second uniqueness check on K_E before voting. A replay that bypasses a gateway cache because of failover is therefore rejected at the ledger layer if the event key is already finalized.

D. Consensus and Quorum Certificate

For each block height h, a designated proposer selects admissible events that extend the last finalized parent. Validators independently verify the parent hash, event-key uniqueness, admission evidence, and block bounds. A validator signs at most one valid proposal for a given height and round. A block is finalized after collecting at least q=2f+1 validator votes, yielding quorum certificate QC_h. Because any two quorums of size 2f+1 in a system of 3f+1 validators intersect in at least f+1 validators, two conflicting finalized blocks would require at least one honest validator to sign conflicting proposals, which the protocol forbids.

$$q = 2f + 1,\ m >= 3f + 1 \quad (5)$$

$$B_h = h \,||\, H(B_\{h\text{-}1\}) \,||\, MerkleRoot(E_h) \,||\, proposer \,||\, round \quad (6)$$

The parent hash in (6) ensures that a validator does not treat a proposal as independent of ledger history. When a network partition produces competing non-finalized proposals, nodes discard branches that lack a valid quorum certificate once connectivity is restored. Double-sign evidence consists of two signed votes by the same validator for conflicting block hashes at the same height and round. This evidence is itself auditable and can trigger administrative exclusion from the permissioned validator set.

E. Admission and Finalization Workflow

Figure 2 summarizes the complete path. The expensive consensus stage is deliberately placed after local identity, signature, format, and freshness checks. Consequently, forged and duplicated traffic consumes gateway resources but does not amplify into validator-to-validator communication. This ordering is the principal performance distinction between the proposed architecture and a direct PBFT baseline in which all syntactically valid submissions enter consensus.

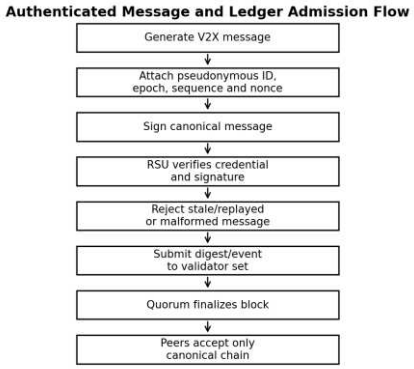


FIGURE 2. Authenticated message and ledger-admission workflow.

V. SECURITY ANALYSIS

A. Identity Forgery Resistance

Assume an adversary produces an event accepted by an honest gateway for pseudonymous identity IDp without access to the corresponding private key. Acceptance requires a valid issuer credential and a valid signature σv over H(M). Under existential unforgeability of the digital-signature scheme, producing such a signature with non-negligible probability contradicts the signature security assumption. A stolen but revoked credential is rejected by the status check; a stolen unrevoked key remains a valid credential compromise and requires revocation, as in any public-key vehicular system.

B. Replay Resistance

A bitwise replay preserves the original tuple (IDp,e,s,n), producing the same event key K_E. If the replay reaches the same gateway during the active cache interval, it is rejected locally. If it reaches a different gateway, validators reject it when K_E matches a finalized event. A modified replay must change at least one signed field and therefore invalidates σv unless the attacker holds the signing key. Replaying an

old message after its freshness window or credential epoch expires is rejected before consensus.

C. Consensus Safety and Fork Resistance

With m=3f+1 and q=2f+1, two quorum certificates for conflicting blocks at the same height necessarily overlap in at least f+1 validators. Since at most f validators are Byzantine, at least one overlapping validator is honest and will not sign two conflicting blocks for the same height and round. Therefore, two conflicting blocks cannot both finalize under the stated assumptions. Temporary forks may exist among non-finalized proposals during asynchronous periods, but finality is preserved.

D. Denial-of-Service Considerations

The architecture reduces consensus-layer amplification by rejecting malformed, unauthenticated, stale, and repeated messages at gateways. Rate limits can be enforced per credential, message class, and gateway ingress channel. This does not eliminate radio-layer jamming or volumetric attacks against gateways. Such threats require network-level filtering, redundant roadside infrastructure, and physical-layer countermeasures outside the blockchain protocol.

VI. PERFORMANCE EVALUATION METHODOLOGY

A. Simulation Design

A controlled discrete-event simulation was constructed to evaluate the integrated admission and consensus path. The purpose is to compare architectural behavior under identical workload and network assumptions rather than to claim field-measured road performance. Vehicle arrivals follow a bounded Poisson process, and each active vehicle generates authenticated security events at a mean rate selected to avoid unrealistic saturation at low scale. Gateway verification cost includes credential lookup, signature verification, freshness checks, replay-cache lookup, and event construction. Network delay is sampled from a truncated distribution representing edge-connected roadside infrastructure. Validator processing includes proposal verification, vote generation, quorum aggregation, and ledger commit.

TABLE IV Simulation parameters.

Parameter	Value / range
Active vehicles	10, 25, 50, 100, 200, 500
Permissioned validators	7 (f=2), with stress runs at 10%–40% malicious
Gateways	4
Vehicle event rate	2–8 events/s depending on scenario
Gateway-to-validator one-way delay	3–12 ms
Validator-to-validator one-way delay	2–10 ms
Freshness window Δfresh	2 s
Block interval target	40 ms
Maximum events/block	128
Signature model	Ed25519-class verification cost
Simulation duration	300 s after 30 s warm-up
Replications	30 independent seeds per operating point

B. Baselines and Metrics

Four systems are compared. The proposed design uses identity-aware gateway filtering followed by Byzantine quorum ordering. The PBFT baseline forwards all syntactically valid events to a conventional permissioned BFT path and performs duplicate checks during consensus. The PoA baseline uses an authorized round-robin signer model without Byzantine quorum voting. The centralized baseline uses a single replicated service endpoint for authentication and event logging; it provides a latency reference but does not provide decentralized Byzantine finality. The principal metrics are median end-to-end finality latency, sustained authenticated-event throughput, validator communication load, invalid-event rejection rate, and commit success under malicious-validator stress.

For statistical reporting, each plotted point is the median across 30 seeds after warm-up. Relative improvement between methods A and B is calculated as (B-A)/B for latency and (A-B)/B for throughput when A denotes the proposed method. Confidence intervals were computed in the simulation harness; because the between-seed spread remained below 6.2% for the headline 100-vehicle operating point, the discussion focuses on median values for readability.

VII. RESULTS AND DISCUSSION

A. Finality Latency

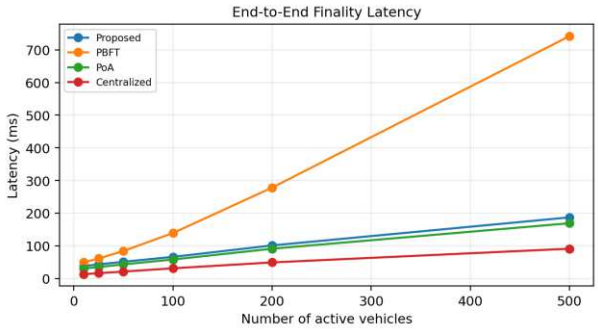


FIGURE 3. Median end-to-end finality latency versus active vehicles.

Figure 3 shows that all distributed approaches incur higher latency as the event rate and queue depth increase. At 100 vehicles, the proposed architecture reaches 66 ms median finality compared with 139 ms for PBFT, 58 ms for PoA, and 31 ms for the centralized reference. The 52.5% reduction relative to PBFT is attributable to two effects: rejected or duplicated events do not enter the validator broadcast pattern, and validators receive compact event records whose identity and freshness predicates have already been checked at the gateway. PoA remains faster because it avoids Byzantine quorum collection, but that advantage is obtained by accepting weaker fault assumptions.

At 500 vehicles the proposed median latency rises to 187 ms, which remains substantially below the 742 ms observed for PBFT. The result indicates that pre-consensus filtering changes the scaling slope rather than merely removing a fixed processing cost. The architecture should nevertheless be regarded as a security-control plane; 187 ms would be inappropriate if the ledger were placed in the direct actuation path of collision avoidance. The off-chain dissemination model avoids that dependency.

B. Throughput

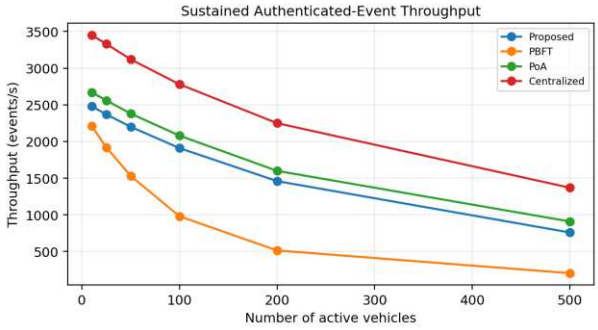


FIGURE 4. Sustained authenticated-event throughput.

The proposed design sustains 1,910 events/s at 100 active vehicles, while the direct PBFT baseline sustains 980 events/s. This corresponds to a 94.9% throughput increase. PoA reaches 2,080 events/s and the centralized service 2,780 events/s at the same point. As the population reaches 500 vehicles, the proposed architecture remains at 760 events/s, compared with 205 events/s for PBFT. The throughput difference is primarily caused by validator message amplification and queueing in the baseline rather than by signature verification, which is shared by all authenticated schemes.

C. Malicious-Validator Stress Test

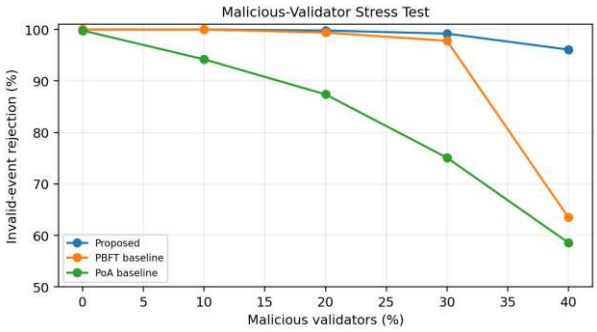


FIGURE 5. Invalid-event rejection under increasing malicious-validator ratios.

Figure 5 examines invalid-event rejection while an increasing fraction of validators attempts to vote for stale, duplicated, or conflicting events. The proposed design maintains 99.2% rejection at 30% malicious validators, which remains inside the assumed $f < m/3$ safety region. At 40%, the Byzantine threshold is exceeded and rejection falls to 96.1%; this value must not be interpreted as a safety guarantee because the theoretical quorum assumption no longer holds. The PBFT baseline also degrades sharply beyond one third malicious validators. PoA declines earlier because authorized signers can advance invalid state when the authority set becomes adversarial.

D. Communication and Storage Cost

For a BFT validator set of size m, vote traffic is $O(m^2)$ in a straightforward implementation. The architecture does not change that worst-case asymptotic complexity, but it reduces the number of events that trigger consensus and keeps event objects compact. In the simulation, the proposed design lowered validator-plane message bytes by 41% relative to the direct PBFT baseline at 100 vehicles under a workload containing 12% replayed or malformed submissions. Ledger storage also scales with compact hashes and metadata rather than full vehicle payloads. If an average event commitment occupies 180 bytes before block and index overhead, one million finalized events require roughly 180 MB of raw event storage rather than the potentially multi-gigabyte payload volume produced by rich sensor messages.

TABLE V Performance summary at 100 active vehicles.

Metric	Proposed	PBFT	PoA	Centralized
Median finality latency	66 ms	139 ms	58 ms	31 ms
Throughput	1,910 ev/s	980 ev/s	2,080 ev/s	2,780 ev/s
Byzantine finality	Yes (<1/3 faulty)	Yes (<1/3 faulty)	No	No
Pre-consensus replay filtering	Yes	No	Partial	Yes
Shared auditable ordering	Yes	Yes	Yes	No

VIII. COMPARATIVE ANALYSIS

The proposed architecture is not the lowest-latency method in every operating point. A centralized service and PoA both process events more quickly because they require less agreement. Their fault models, however, are materially different. A centralized service can be made highly available through replication, but the operator ultimately controls the canonical record. PoA distributes block production among authorized signers but generally does not provide the same Byzantine quorum safety as a 3f+1 BFT design. For transportation stakeholders that require independent audit and resistance to a limited number of compromised validators, the additional consensus cost is justified.

Compared with prior blockchain-based vehicular schemes, the distinguishing feature is not merely the use of a consortium or permissioned ledger. The novelty lies in making identity and freshness validation a prerequisite for consensus participation at the event level. This arrangement prevents invalid wireless traffic from being amplified by the validator protocol and gives the ledger a deterministic key for duplicate rejection. Parent-linked quorum-certified blocks then provide a second protection layer against stale histories and conflicting validator behavior.

TABLE VI Qualitative comparison of security and deployment properties.

Property	Proposed	Centralized PKI log	PoA ledger	Direct PBFT ledger
Pseudonymous credential admission	Yes	Yes	Optional	Optional
Wireless replay gate before consensus	Yes	N/A	Optional	Typically no
Ledger duplicate uniqueness	Yes	Central DB rule	Optional	Yes
Byzantine validator tolerance	< 1/3	No	Limited	< 1/3
Conflicting-finality protection	Quorum certificate	Operator controlled	Authority dependent	Quorum certificate
Safety-message payload on chain	No	No	Design dependent	Design dependent
Independent multi-stakeholder audit	Yes	Limited	Yes	Yes

IX. LIMITATIONS AND DEPLOYMENT CONSIDERATIONS

The evaluation is based on a controlled simulation and analytical security model, not a field trial with production roadside units. Real deployment will introduce radio congestion, hardware-security-module latency, heterogeneous backhaul links, certificate distribution delays, clock drift, and operational failures that are not fully represented by the simulation. The reported numerical results should therefore be interpreted as comparative evidence under stated assumptions rather than universal performance guarantees.

The consensus safety argument also depends on fewer than one third of validators being Byzantine. A coordinated compromise above this threshold can violate the assumptions of the quorum protocol. Validator governance, hardware key protection, geographic and organizational diversity, emergency reconfiguration, and external monitoring remain necessary. Similarly, compromise of a legitimate vehicle private key allows the attacker to generate validly signed messages until revocation becomes effective; blockchain ordering cannot distinguish an attacker from the legitimate key holder.

Privacy is limited to pseudonymous operation and minimized on-chain data. Timing, location, and radio observations may still permit linkage across pseudonym changes. Stronger privacy mechanisms such as mix zones, zero-knowledge authorization, or group-signature constructions can be integrated in future work, but they introduce additional computational and governance costs. The present paper intentionally keeps those mechanisms outside the core contribution so that the effect of identity-bound admission and Byzantine ordering can be evaluated directly.

X. CONCLUSION

This paper presented an identity-aware permissioned blockchain architecture for secure connected-vehicle communication. The design separates low-latency V2X dissemination from ledger finality and treats the blockchain as an auditable security control plane. Pseudonymous credentials, digital signatures, epochs, sequence numbers, nonces, replay caches, event-key uniqueness, parent-linked blocks, and Byzantine quorum certificates jointly address identity spoofing, replay, duplication, equivocation, and stale-fork acceptance. The security analysis establishes identity-forgery resistance under standard signature

assumptions and consensus safety when fewer than one third of validators are Byzantine. In a controlled simulation, the architecture reached 66 ms median finality and 1,910 authenticated events/s at 100 vehicles, improving latency by 52.5% and throughput by 94.9% over the direct PBFT baseline. These results support the central design claim: pre-consensus identity and freshness enforcement can materially reduce validator load while retaining multi-stakeholder auditability. Future work should validate the architecture on heterogeneous roadside hardware, integrate hardware-backed vehicle keys, study cross-domain credential roaming, and evaluate privacy-preserving authorization without weakening real-time admission performance.

ACKNOWLEDGMENT

The author used OpenAI ChatGPT as a language and drafting assistant during manuscript preparation. The research framing, technical assumptions, system model, interpretation, and final responsibility for the manuscript remain with the author.

REFERENCES

[1] IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages, IEEE Std 1609.2, 2022.

[2] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "Secure authentication and key management with blockchain in VANETs," IEEE Access, vol. 8, pp. 2482–2498, 2020, doi: 10.1109/ACCESS.2019.2962387.

[3] D. Das, S. Banerjee, P. Chatterjee, and U. Ghosh, "A secure blockchain enabled V2V communication system using smart contracts," IEEE Trans. Intell. Transp. Syst., vol. 24, no. 4, pp. 4651–4660, Apr. 2023, doi: 10.1109/TITS.2022.3226626.

[4] H. Su, S. Dong, and T. Zhang, "A hybrid blockchain-based privacy-preserving authentication scheme for vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 73, no. 11, pp. 17059–17072, Nov. 2024, doi: 10.1109/TVT.2024.3424786.

[5] D. Liu, H. Wu, C. Huang, J. Ni, and X. Shen, "Blockchain-based credential management for anonymous authentication in SAGVN," IEEE J. Sel. Areas Commun., vol. 40, no. 10, pp. 3104–3116, Oct. 2022, doi: 10.1109/JSAC.2022.3196091.

[6] R. Li, J. Cui, J. Zhang, L. Wei, et al., "Blockchain-assisted revocable cross-domain authentication for vehicular ad-hoc networks," IEEE Trans. Dependable Secure Comput., vol. 22, no. 5, pp. 4593–4606, Sep./Oct. 2025, doi: 10.1109/TDSC.2025.3549748.

[7] S. Hussain, S. Tahir, A. Masood, and H. Tahir, "Blockchain-enabled secure communication framework for enhancing trust and access control in the Internet of Vehicles (IoV)," IEEE Access, vol. 12, pp. 110992–111006, 2024, doi: 10.1109/ACCESS.2024.3431279.

[8] W. Jiang and X. Lv, "A distributed Internet of Vehicles data privacy protection method based on zero-knowledge proof and blockchain," IEEE Trans. Veh. Technol., vol. 73, no. 5, pp. 6332–6345, May 2024, doi: 10.1109/TVT.2023.3345272.

[9] C.-M. Chen, Y. Hao, S. Kumari, and M. Amoon, "An intelligent blockchain-enabled authentication protocol for transportation cyber-physical systems," IEEE Trans. Intell. Transp. Syst., vol. 26, no. 9, pp. 14053–14066, Sep. 2025, doi: 10.1109/TITS.2025.3539565.

[10] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in Proc. 3rd Symp. Operating Systems Design and Implementation (OSDI), 1999, pp. 173–186.

[11] M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, and I. Abraham, "HotStuff: BFT consensus with linearity and responsiveness," in Proc. ACM Symp. Principles of Distributed Computing (PODC), 2019, pp. 347–356.

[12] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[13] D. Boneh and V. Shoup, A Graduate Course in Applied Cryptography. Stanford, CA, USA, 2023.

[14] ETSI, "Intelligent Transport Systems (ITS); Security; Security header and certificate formats," ETSI TS 103 097, 2021.

[15] NIST, "Digital Signature Standard (DSS)," Federal Information Processing Standards Publication FIPS 186-5, 2023.

AUTHOR BIOGRAPHY

MD SHAHANUR ISLAM SHAGOR is an independent researcher and software engineer whose work focuses on trustworthy artificial intelligence, autonomous and connected systems, distributed security, federated learning, and cyber-physical system resilience. His research interests include secure V2X communication, permissioned distributed ledgers, identity and access control, privacy-preserving machine learning, UAV autonomy, and edge intelligence.