2025 6th International Conference on Communications, Information, Electronic and Energy Systems (CIEES)
26 – 28 November, 2025, Ruse, Bulgaria

Immutable Audit of EV Charging Sessions using Blockchain and IPFS

Nexhibe Sejfuli - Ramadani
Faculty of Natural Sciences and Mathematics
University of Tetova
Tetovo, North Macedonia
nexhibe.sejfuli@unite.edu.mk

Jelena Gjorgjev
Faculty of Informatics
American University of Europe - FON
Skopje, North Macedonia
jelena.gjorgjev1@gmail.com

Valentina Angelkoska
Faculty of Economics
University of Skopje
Skopje, North Macedonia
valentina.angelkoska.utms@gmail.com

Erenis Ramadani
Software Engineer
Tarmac LLC
Tetovo, North Macedonia
erenisramadani@gmail.com

Florim Idrizi
Faculty of Natural Sciences and Mathematics
University of Tetova
Tetovo, North Macedonia
florim.idrizi@unite.edu.mk

Aleksandar Risteski
Faculty of Electrical Engineering and Informations Technologies
Ss. Cyril and Methodius University
Skopje, North Macedonia
acerist@feit.ukim.edu.mk

***Abstract*— As electric vehicles (EVs) become more prevalent, ensuring secure and transparent tracking of their charging activities has emerged as a critical challenge. Traditional centralized methods are vulnerable to data integrity issues and lack resilience, raising concerns about trustworthiness. This work presents a blockchain-enhanced architecture for auditing EV charging sessions. It offloads Charging Data Records (CDRs) to the InterPlanetary File System (IPFS), while preserving their integrity through cryptographic anchors recorded on an Ethereum-compatible smart contract. This approach strikes a balance between decentralization and system performance. A prototype was developed featuring OCPP-based session simulation and automated verification via smart contracts. Experimental evaluation across thousands of test cases confirmed the system's ability to detect data tampering with minimal processing overhead, especially when integrated with Layer-2 scaling technologies. These results demonstrate the framework's potential to improve transparency and trust in EV charging networks.**

Keywords—smart contracts, EV charging, blockchain, OCPP, IPFS

I. Introduction

In the past decade, growing concerns about climate change and environmental pollution have prompted many countries to invest in sustainable technologies for the transportation sector. As a result, Electric Vehicles (EVs) are experiencing rapid adoption in global markets, driven by technological advancements, decreasing battery costs, and government incentives such as tax subsidies and infrastructure support [1].

Alongside the growth in EV adoption, there is a parallel need for the development of smart charging infrastructure, which ensures fast, secure, and traceable energy delivery. A critical component of this infrastructure is the management and logging of EV charging sessions, which involves storing data such as session start and end times, energy consumption, user identification, and billing information [2].

Currently, many of these systems operate on centralized architectures, where the data is stored and controlled by individual charging network operators or energy service providers. However, these centralized models introduce several challenges, including: possible data manipulation, lack of transparency, and the risk of single points of failure [3].

In this context, there is a growing demand for technological solutions that ensure traceability, transparency, and data integrity in a decentralized manner. Blockchain technology, which has gained recognition for its applications in finance and supply chain management, is increasingly being viewed as a promising alternative for addressing these issues in the energy and transportation sectors [4].

Blockchain allows for immutable, distributed, and verifiable data storage, eliminating the need for a centralized authority. When combined with technologies such as the *InterPlanetary File System* (IPFS) for off-chain data storage and smart contracts for automating verification and agreement enforcement, blockchain provides a robust platform for building a trusted system for auditing EV charging sessions [5].

This background justifies the development of a new technological approach aimed at overcoming the limitations of existing systems and introducing security, trust, and scalability in EV charging management.

II. Problem Statement

The worldwide shift toward electric mobility has accelerated considerably, bringing with it not only innovation but also significant challenges in infrastructure development. One critical area of concern is the secure and transparent handling of Electric Vehicle (EV) charging data, particularly in environments where accurate, verifiable, and tamper-resistant records are essential [2].

At present, the majority of EV charging networks operate through centralized architectures. In such systems, service providers or operators retain full ownership over the creation, storage, and management of Charging Data Records (CDRs). This structure introduces several risks, including system-wide failure due to central points of control, potential manipulation of session data by malicious actors, limited transparency for stakeholders, and insufficient support for reliable auditing or conflict resolution [3][4].

979-8-3315-0119-8/25/$31.00 ©2025 IEEE

These challenges become even more pronounced in complex charging scenarios—such as those involving roaming capabilities, collaborations between multiple service providers, or decentralized energy marketplaces—where trust among independent entities is crucial [5].

While cloud-based solutions have been introduced to enhance data security, they still depend on trusted intermediaries and fail to provide decentralized assurance of data validity. Most existing systems also lack the capability to verify data integrity through cryptographic means or to detect unauthorized modifications in real-time [6].

Given these limitations, there is a clear need for a more resilient solution that:

- Guarantees the integrity and immutability of session records;
- Facilitates decentralized verification without relying on central authorities;
- Enables scalable, cost-effective, and transparent auditing procedures;
- Maintains compatibility with current charging communication standards like OCPP [6].

This research proposes a blockchain-enabled architecture designed to address these issues. By leveraging distributed ledger technology alongside decentralized storage and smart contracts, the framework aims to strengthen data integrity, enhance trust, and provide reliable auditability for EV charging networks.

1) Objectives of the Study

Based on the challenges identified in the management and auditing of Electric Vehicle (EV) charging session data, the primary aim of this study is to develop a blockchain-based technical framework that ensures security, transparency, and decentralized verifiability of charging records [2][3].

The proposed system addresses the limitations of current centralized infrastructures by implementing a hybrid architecture, in which detailed *Charging Data Records* (CDRs) are stored off-chain using systems like the *InterPlanetary File System (IPFS)* [4], while essential metadata and cryptographic hashes are securely anchored on Ethereum-compatible smart contracts [5].

The specific objectives of this study are:

1) Analyze the limitations of the current architectures: Analyze the current limitations of centralized architectures in storing and verifying *Charging Data Records (CDRs)* within EV charging infrastructures [3].

2) Decentralized framework design: To design a decentralized framework that integrates blockchain, IPFS and smart contracts to ensure data immutability and traceability [5].

3) Implement a prototype: To implement a functional prototype that includes:

a) An OCPP-based charging session simulator [6].

b) A component for generating and pinning CDR hashes to IPFS

c) A smart contract responsible for session anchoring and integrity verification [5].

4) System performance evaluation: To evaluate the system's performance under large-scale simulated conditions (e.g. thousands of charging sessions) by measuring:

a) Verification latency

b) Blockchain transaction cost

c) System's ability to detect data manipulation [5].

This study aims to contribute toward enhancing data integrity and trust in EV charging infrastructures by offering an innovative solution for automated and decentralized auditing of charging sessions.

2) Significance of the study

The rapid global shift toward electric mobility has created an urgent need for secure, transparent, and scalable systems that can ensure the trustworthiness of Electric Vehicle (EV) charging transactions. As EV adoption increases, maintaining the integrity of charging data becomes vital—not only for service providers and network operators but also for end-users and regulatory bodies [1][2].

Traditional EV charging systems often rely on centralized architectures, which introduce vulnerabilities such as data tampering, single points of failure, and limited auditability. These challenges are particularly critical in environments that require high levels of trust, such as roaming scenarios, cross-provider settlements, and peer-to-peer energy exchanges [3]. In this context, the use of blockchain and decentralized storage technologies offers a compelling alternative.

1) Technological Innovation: The research introduces a novel hybrid architecture that integrates blockchain with off-chain storage systems (e.g., IPFS) to achieve data immutability, traceability, and tamper resistance, without overloading the blockchain. This contributes to the broader discourse on blockchain scalability and efficiency in the energy sector [4][5].

2) Improved Data Security and Trust: By employing Ethereum-compatible smart contracts for session anchoring and verification, the system offers cryptographic guarantees for data integrity. This enhances trust among independent stakeholders and addresses key concerns in EV roaming and billing transparency [3][5].

3) Scalability and Efficiency: The use of Layer-2 solutions enables faster and lower-cost transactions, overcoming limitations traditionally associated with blockchain networks. This supports the feasibility of real-time and large-scale deployment in future EV charging ecosystems [5].

4) Compatibility with Existing Standards: The prototype developed in this research is built around the Open Charge Point Protocol (OCPP), ensuring practical relevance and interoperability with existing charging infrastructure [6].

5) Contribution to Academic and Industry Advancement: The results of this study can inform both academic research and industrial development in the fields of smart mobility, energy informatics, and decentralized systems. It lays the groundwork for future implementations that address legal compliance, real-world integration, and cross-border EV infrastructure.

In summary, this research addresses a critical gap in the secure and auditable management of EV charging data. It contributes a functional, scalable, and standards-compliant solution that aligns with the evolving demands of smart mobility infrastructure.

III. System Architecture And Component Design

1) First Component: OCPP Backend – Data Acquisition and Charging Coordination

At the core of the physical infrastructure lies the OCPP backend, which acts as a Charge Station Management System (CSMS). Its primary responsibility is to interface with distributed EV chargers and orchestrate user interactions using standardized message types such as Authorize, StartTransaction, MeterValues, StopTransaction, and RemoteStart [7].

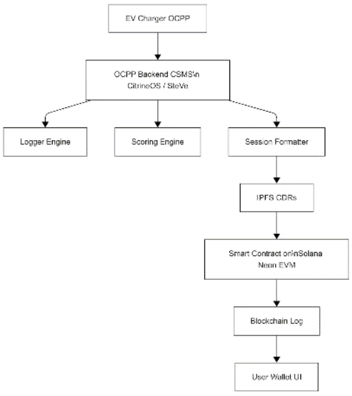

Fig. 1: System Architecture for Immutable Auditing of EV Charging Sessions

The diagram in Fig. 1 presents the end-to-end system architecture of the proposed EV charging audit framework. The system begins with OCPP-enabled EV chargers connected to a backend management system. Session logs are evaluated, scored, and securely stored in IPFS, while metadata and hashes are anchored on a smart contract deployed on a Solana-based EVM-compatible blockchain. The blockchain acts as a public, immutable ledger for verification purposes. Users interact through EVM wallets, ensuring accountability and transparency.

Unlike monolithic solutions, the system leverages a microservice-based OCPP backend that decouples charger communication from higher-order logic such as user scoring, session settlement, and reward processing. Event-driven architectures, using message queues like Apache Kafka or RabbitMQ, are recommended to allow the backend to emit asynchronous hooks to downstream components when critical session events occur. These include reservation confirmations, charging starts, mid-session meter readings, and transaction terminations [8][9].

By integrating open-source frameworks such as *CitrineOS* or *SteVe*, the backend supports OCPP versions 1.6 and 2.0.1. The latter is particularly valuable for its enriched transaction events and support for advanced features such as smart charging profiles, tariff classes, and reservation windows [7][10].

2) Second Component: Behavior Scoring and Reputation Module

The behavioral scoring engine functions as the cognitive layer of the system, transforming raw operational data into semantically rich assessments of user behavior. Inspired by the design of reputation systems in digital energy networks, the module applies a set of policy-driven rules to compute score deltas—positive or negative—based on users' compliance with predefined operational guidelines [7][8].

Session logs forwarded from the OCPP backend are ingested, validated, and assessed across several behavioral dimensions:

- Arrival punctuality: Users arriving later than their reserved charging slot are penalized to discourage station blocking and improve scheduling reliability [8].
- Peak-hour compliance: Charging sessions during high-demand periods are monitored, and excessive energy use incurs deductions to reduce grid strain [9].
- Idle time post-charging: Users who leave their vehicle connected after charging ends are penalized to optimize station availability and fairness [7][8].
- Energy efficiency: Positive reinforcement is awarded to users whose session utilization exceeds predefined efficiency thresholds (e.g., >80%) [8].

These scoring rules reflect both operational efficiency and grid-aware behaviors. The module supports configurable rule weights, allowing station operators or utility providers to prioritize behavior dimensions based on local grid constraints, demand forecasts, or environmental policies [9].

Table 1: Behavior Scoring Table for EV Charging Sessions

No.	Evaluated Behavior	Description	Score ±
1	**Late Arrival**	User arrives after their reserved time slot	–5
2	**Idle After Charging**	Vehicle remains connected after charging is complete	–3
3	**Charging During Peak Hours**	Charging during periods of high grid demand	–2
4	**Charging Efficiency >80%**	Session uses >80% of reserved time for actual charging	+5
5	**Use of Smart Charging Profiles**	Complies with pre-configured smart energy profiles	+3
6	**Reservation Cancellation Without Notice**	User cancels just before the session begins	–4
7	**Correct Tariff Selection**	Chooses tariffs that optimize cost and grid stability	+2

This table presents the scoring rules used to evaluate user behavior during EV charging sessions. Each rule represents either a penalty (–) or reward (+), designed to promote grid-friendly, efficient, and fair use of charging infrastructure. The rules can be customized by operators depending on policy and energy constraints.

Future iterations of the system may integrate adaptive machine learning models such as clustering-based user profiling or reinforcement learning to dynamically adjust scoring rules and detect behavior trends over time [10].

3) Third Component: Blockchain and Smart Contract Layer

To preserve data immutability, trust, and verifiability, final score updates and session proofs are committed to a smart contract deployed on a Solana-based EVM-compatible blockchain. While Ethereum remains a widely used platform for smart contract deployment, this system leverages Neon EVM on Solana, offering significantly lower transaction fees while maintaining compatibility with Ethereum tooling such as MetaMask and Solidity [11][12].

The illustration in Fig. 2 shows the life cycle of a charging session within the proposed blockchain-based auditing system. The process begins with a reservation, followed by session execution. Behavioral metrics are evaluated post-session, with Charging Data Records (CDRs) stored in IPFS and cryptographic metadata anchored on a smart contract deployed on a Solana-based EVM chain. The user score is updated and stored immutably.

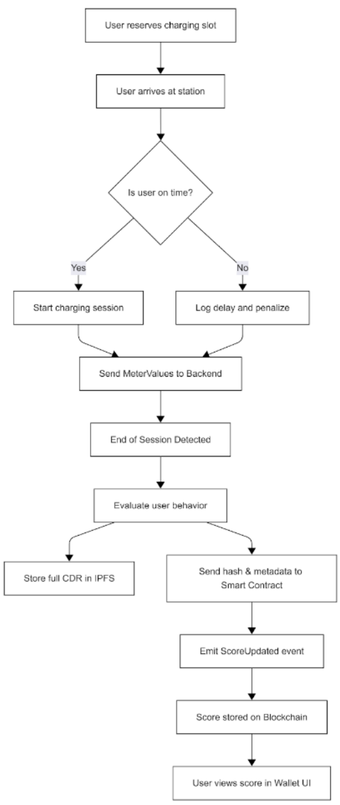

Fig. 2: Flow Diagram of a Charging Session in the Immutable Audit System

1) Contract Logic and Storage Model: The smart contract exposes core functions such as:

function updateScore (address user, ChargingSession session) public;

The ChargingSession struct encapsulates various behavior metrics, including:

- Arrival delay
- Idle time
- Peak-hour flag
- Session efficiency

Upon invocation, the smart contract emits a *ScoreUpdated* event and updates the *mapping(address => int)* storage accordingly.

To remain gas-efficient, the contract avoids complex logic on-chain. Instead, the scoring computation is performed off-chain, and the contract acts as a verifier and state registrar. This architectural decision aligns with best practices in gas optimization and minimal trust assumptions [13].

2) Identity and Signature Flow: Users interact with the contract using EVM-compatible wallets. Each charging session is linked to a unique wallet address, which serves as a persistent identity and provides non-repudiation.

During a session initiation, users may be required to sign a confirmation message, such as: *"I agree to start session X at time Y"*. These signed messages are cryptographically verifiable and can serve as evidence for audits and dispute resolution [14].

To reduce friction, the system optionally supports meta-transactions, where a gas relayer (e.g., station operator) submits transactions on behalf of users. This pattern ensures that users can interact with smart contracts without holding native tokens, while the station may recover transaction fees during post-session billing [15].

The smart contract layer represents a fundamental component in the proposed system architecture, ensuring the integrity, transparency, and auditability of EV charging session data. By anchoring behavior-related metadata and cryptographic hashes onto an immutable blockchain, the contract serves as a trusted and tamper-resistant ledger. Integration with widely adopted Ethereum tools such as MetaMask, and deployment via Neon EVM on the Solana network, enables low-cost transactions without sacrificing EVM compatibility. Furthermore, support for meta-transactions lowers entry barriers for end users, offering a more inclusive and accessible user experience.

Looking forward, this layer can be extended to include upgradeable contract patterns, role-based access control (RBAC), and advanced privacy-preserving techniques such as zero-knowledge proofs. These enhancements would further strengthen the system's security, scalability, and compliance with evolving regulatory and technical requirements.

IV. Scope and Limitations

This research focuses on designing and evaluating a hybrid blockchain-based framework for secure and verifiable auditing of Electric Vehicle (EV) charging sessions. The scope is limited to the technical aspects of data integrity, session traceability, and decentralized verification using smart contracts and off-chain storage.

Despite its contribution, the proposed system has certain constraints that must be acknowledged:

1) Simulation-Based Testing: The evaluation is performed using simulated charging sessions. While the results provide useful insights, real-world implementation may involve additional factors such as network reliability, hardware integration, and operational policies.

2) Scalability in Real Networks: Although Layer-2 solutions are considered, the framework has not been deployed or tested in high-traffic, production-scale EV networks, where scalability, interoperability, and latency may vary.

3) Security Assumptions: The framework assumes that the underlying blockchain and IPFS systems are trustworthy and functional. Attacks on IPFS nodes, Ethereum forks, or smart contract vulnerabilities are not explicitly mitigated.

4) Regulatory and Legal Aspects: This study does not address the legal, privacy, or regulatory implications of storing and processing EV charging data on decentralized platforms, which may vary across jurisdictions.

By acknowledging these limitations, the study maintains a clear boundary of its contributions and provides a foundation for future work aimed at extending the framework toward real-world deployment, interoperability, and legal compliance.

V. Conclusion

This study presented an integrated framework for achieving immutable, transparent, and decentralized auditing of Electric Vehicle (EV) charging sessions. By combining an OCPP-based backend for real-time data acquisition, a behavioral scoring module for evaluating user conduct, and a blockchain-powered smart contract layer for anchoring session metadata, the system addresses critical challenges related to trust, verifiability, and data integrity in modern EV infrastructure.

The proposed architecture leverages the InterPlanetary File System (IPFS) for efficient off-chain storage of Charging Data Records (CDRs), while maintaining cryptographic proofs and metadata on a cost-efficient EVM-compatible blockchain. This design ensures tamper resistance without compromising performance or user accessibility.

Through modular and scalable components, the system facilitates user accountability, supports interoperable protocols like OCPP 1.6 and 2.0.1, and promotes behavioral incentives through a transparent scoring and reward mechanism. Additionally, features such as meta-transactions and wallet-based identity enhance usability and inclusiveness, even for users without direct access to native blockchain tokens.

In conclusion, this work demonstrates that distributed ledger technologies, when thoughtfully integrated with EV charging ecosystems, can significantly improve transparency, efficiency, and trustworthiness. Future developments may include advanced privacy-preserving mechanisms, integration with real-world charging infrastructure, and adaptive machine learning models to further personalize and optimize user behavior in energy-conscious environments.

References

[1] International Energy Agency, "Global EV Outlook 2023." [Online]. Available: https://www.iea.org/reports/global-ev-outlook-2023.

[2] M. M. Rahman, K. Ko, and H. Yoon, "A survey on blockchain for electric vehicle charging and integration with smart grid," Renewable and Sustainable Energy Reviews, vol. 137, p. 110618, 2021, doi: 10.1016/j.rser.2020.110618.

[3] M. H. Rehman, K. Salah, E. Damiani, and R. Jayaraman, "Blockchain-based smart contract for EV charging management," in Proc. IEEE Int. Conf. Commun. (ICC), Dublin, Ireland, 2020, pp. 1–6, doi: 10.1109/ICC40277.2020.9148959.

[4] M. Andoni et al., "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," Renewable and Sustainable Energy Reviews, vol. 100, pp. 143–174, 2019, doi: 10.1016/j.rser.2018.10.014.

[5] S. Chakraborty, P. K. Das, A. Roy, and S. K. Das, "Blockchain-based secure and trusted energy transaction framework for electric vehicles in smart cities," IEEE Trans. Ind. Informat., vol. 17, no. 6, pp. 4291–4298, Jun. 2021, doi: 10.1109/TII.2020.3013605.

[6] Open Charge Alliance, "OCPP – Open Charge Point Protocol," 2023. [Online]. Available: https://www.openchargealliance.org/

[7] M. F. Shaaban, E. F. El-Saadany, and A. M. Youssef, "A framework for decentralized demand response in smart grid using autonomous electric vehicles," IEEE Trans. Smart Grid, vol. 7, no. 2, pp. 1119–1129, Mar. 2016, doi: 10.1109/TSG.2015.2424708.

[8] C. Zhang, J. Wu, C. Long, and M. Cheng, "Review of existing peer-to-peer energy trading projects," Energy Procedia, vol. 105, pp. 2563–2568, 2017, doi: 10.1016/j.egypro.2017.03.737.

[9] B. Hu, Y. Zhou, Z. Qian, and L. Su, "A behavior-aware EV charging management system using reputation scoring," in Proc. IEEE Int. Conf. Commun. (ICC), 2019, pp. 1–6, doi: 10.1109/ICC.2019.8761312.

[10] M. Gharavi and R. Ghafurian, "Smart grid: The electric energy system of the future," Proc. IEEE, vol. 99, no. 6, pp. 917–921, Jun. 2011, doi: 10.1109/JPROC.2011.2114650.

[11] Neon Labs, "Neon EVM: Ethereum on Solana," 2023. [Online]. Available: https://neonlabs.org/

[12] Solana Foundation, "Solana: Scalable blockchain for decentralized apps," 2023. [Online]. Available: https://solana.com/

[13] G. Wood, "Ethereum: A secure decentralized transaction ledger," Ethereum Yellow Paper, 2022. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf

[14] A. Mavridou and A. Laszka, "Designing secure Ethereum smart contracts: A finite state machine based approach," in Proc. IEEE Int. Conf. Software Quality, Reliability and Security (QRS), Lisbon, Portugal, 2017, pp. 418–423, doi: 10.1109/QRS.2017.47.

[15] ConsenSys, "Meta-transactions and gasless onboarding," 2022. [Online]. Available: https://consensys.net/blog/developers/how-meta-transactions-work/.