System proposal for integration of offline blockchain payment models in a fully offline EV authentication and charging procedure

Nexhibe Sejfuli-Ramadani [1,4]
[1] Faculty of Natural Sciences and Mathematics
University of Tetova, N. Macedonia
nexhibe.sejfuli@unite.edu.mk

Jelena Gjorjev [2,4]
[2] Faculty of Informatics
American University of Europe – FON,
Skopje, N. Macedonia
jelena.gjorgjev@fon.edu.mk

Valentina Angelkoska [3]
[3] Faculty of Economics
University of Skopje
Skopje, N. Macedonia
valentina.angelkosa.utms@gmail.com

Florim Idrizi [1]
[1] Faculty of Natural Sciences and Mathematics
University of Tetova,
Tetovo, N. Macedonia
florim.idrizi@unite.edu.mk

Marko Porjazoski [4]
[4] Faculty of Electrical Engineering and Information Technologies
Ss. Cyril and Methodius University in Skopje, N. Macedonia
markop@feit.ukim.edu.mk

Aleksandar Risteski [4]
[4] Faculty of Electrical Engineering and Information Technologies
Ss. Cyril and Methodius University in Skopje, N. Macedonia
acerist@feit.ukim.edu.mk

***Abstract*— This paper proposes a model for offline payment in electric vehicle (EV) charging systems, integrating an authentication based on license plates with payment using SMS-based transactions or NFC communication. By proposing a new model, we explore the synergy of smart contracts with these technologies, aiming to provide seamless authentication, handle charging tariffs, calculate rewards, and ensure a secure and automated payment process without relying on continuous internet connectivity.**

Keywords—blockchain, electric vehicle, charging, offline, payment, smart contract

I. INTRODUCTION

As electric vehicles (EVs) pose a great eco-friendly mode of transportation, numerous countries are devising strategies to motivate more individuals to turn to this sustainable mode of transportation. Since January 2022, even the U.S. Bank introduced credit card incentives tailored for EV owners [1], where they get back a percentage of the sum paid for a charging session. Within a span of less than two years, six other major banks followed suit [2], recognizing the growing significance of electric vehicles, but there are still some challenges that need to be overcome, especially in the area of payment for charging services and distribution of funds among the stakeholders.

In a study that outlines the new blockchain-based charging system, the researchers at the University of Waterloo found that there is a lack of trust among charging service providers, property owners and owners of electric vehicles [3]. The EV supply equipment is operated by the charging service provider, so the property owners must trust the provider to compensate them fairly for the electricity used.

Also, when someone wants to charge their electric vehicle at another person's outlet, they can't just pay that person directly. Instead, they need a middleman system. This means electric vehicle owners must sign up with many charging companies, and guests can't easily pay for the power they use [4].

All these issues can be overcome by introducing blockchain into the EV charging process. Many have studied this approach, achieving not only secure EV charging systems that are based on blockchain technology [4][5][6], but also EV Charging Management Systems [7][8] for managing power distribution grids.

However, making payments with blockchain technology requires an internet connection, and there are areas where this is a problem, like in remote locations or during network outages, individuals might not have internet access to pay for parking services that requires online payment methods.

The paper is organized as follows: in Section II, we present the problems that blockchain-based systems face in specific circumstances where internet connection is not available, some of the existing technologies that can help solve these problems and their advantages/disadvantages. as well as what we think will work best for the described situations. In Sections III and IV we present a new model where we combine what we think are the most efficient solutions for subproblems of the offline payment in an EV offline authentication and charging model. Potential risks are identified and their management is briefly discussed in Section V. Finally, we conclude the paper in Section VI.

II. OFFLINE CHARGING PROBLEM

Typical places where internet connection is extremely weak or even not available are underground garages. Rural areas, areas shadowed by buildings, premises where a considerable amount of electronic equipment is used, such as hospitals, medical facilities, industrial areas, factories, etc. are also places where communication signals suffer major attenuation and interference. The fact that users may

not always have available Internet connection makes it challenging to have blockchain based EV charging systems easily accessible.

However, blockchain transactions are a form of individual-to-individual agreement that does not involve an authorized third party that handles the security aspect (like bank systems do), so offline payment is difficult, because the person that pays, has to initialize the transaction with the required transaction data, which is a process that needs an internet connection. Therefore, there are two problems that arise when thinking of potential offline payment models: Offline authentication and offline payment.

An authentication method employed by most charging stations is Radio-Frequency Identification (RFID). Users can authenticate themselves by simply tapping or swiping their RFID cards at the charging station [9]. However, implementing an RFID card system requires manufacturing and distributing physical cards, coupled with the installation of RFID readers at charging stations. The administrative tasks associated with issuing, replacing, and revoking cards add further complexity. Also, different RFID card systems may not be compatible with each other. If a user has an RFID card from one vendor, it might not work with charging stations from another vendor, limiting interoperability.

Modern electric vehicles come equipped with built-in authentication systems, including telematics systems, NFC, or Bluetooth communication. These mechanisms enable vehicles to transmit unique identifiers directly to the charging station, paving the way for a more seamless and automatic authentication process, potentially integrated into a smart contract. However, additional security layers are required to safeguard the uncorrupted transmission of identifiers. This necessity introduces complexity to the smart contract code and increases deployment costs.

A. Offline Authentication

A potential solution for offline authentication has already been proposed. In January 2023, a student in the University of Zurich created a hands-free, fully automated, and shared usage of a low-power portable EV home charger [10]. Basically, they connected an EV charger to a camera system that would detect and identify cars by their license plate. This ensured a fully automated and hands-free triggering and authentication process without any human intervention and that, most importantly, doesn't require internet connection.

Although the project was created for Switzerland's network problems in some garages and to avoid administrative and security measures of high-power charges, it has the potential to solve two crucial problems of EV charging systems:

- Provide a simple, universal identifier (license plates) that, even if external mechanisms or applications are used, it would simplify their algorithm;
- Transmit data through wires, removing huge security layers that are currently necessary because of our existing options for user identification, making the system simpler, more efficient, and faster.

One potential risk that should be handled here is special authorization to employees to input the license plate manually in case there is an eventual problem where the camera cannot read or identify it properly.

B. Offline Payment

The offline payment problem has two stages: user identification and transaction initiation. User identification can be solved in a similar way to using the RFID: all modern smartphones have NFC modules that can be used to transmit data wirelessly in very short distances (for security reasons). By bringing an NFC-enabled device close to NFC reader, the transaction details can be recorded and processed on a blockchain network [11]. The NFC reader captures the transaction data and sends it to the smart contract. This data packet could contain the user's identity (license plate), payment details (amount paid), and any other relevant information required by the smart contract. This method allows secure, fast, and convenient transfers without the need for an internet connection at the point of transaction.

Transaction initiation can be solved by another pioneering field of research: using SMS messages to make blockchain transactions, with software products like Samourai Wallet [12] for Bitcoin and MEW Offline [13] for Ethereum, that also offer full online wallet support for crypto users. These are specialized services that allow for blockchain transactions via SMS. The SMS messages contain a hash or other identifier that corresponds to a transaction on the blockchain. This identifier can serve as proof of payment. Upon receiving an SMS with the transaction identifier, the smart contract can verify the transaction on the blockchain to ensure that the payment was successful. However, it's important to have a backup verification process, such as manually checking the transaction status.

Another way is for users to scan a QR code with Samourai Wallet (SW) or MEW Offline (MO) to sign transactions. This could be displayed on a dedicated screen at the charging station. After scanning the QR code, SW/MO signs the transaction offline, ensuring that the private key never leaves the user's device. Once the transaction is signed, a signature that can be submitted to the blockchain will be provided. This signature is then used by the smart contract to verify and record the transaction.

An ideal consensus protocol should prioritize security, low energy usage, and high transaction speed while being less reliant on real-time online connectivity due to potential limitations in remote charging locations or network downtimes. Here are two appropriate consensus mechanisms [14]:

- Proof of Authority (PoA) is a consensus process used in private or consortium

blockchains where approved accounts, called validators, validate transactions and blocks. Proof of Authority (PoA) is quicker and more energy-efficient than Proof of Work (PoW), making it ideal for situations requiring rapid transactions, as in an electric vehicle charging setting. Its centralized nature may not be compatible with many decentralized applications.

- Proof of Stake (PoS) Versions: Proof of Stake (PoS) and its derivatives such as Delegated Proof of Stake (DPoS) or Leased Proof of Stake (LPoS) are options to be evaluated for their energy efficiency and quicker transaction processing capacity. These protocols offer a more decentralized method compared to PoA and may be tailored to facilitate offline transaction signing, where a transaction is signed offline and sent by SMS for confirmation.

III. New Model Using License Plate-Based Authentication and NFC or SMS Payment

Integrating a smart contract with a camera system at an EV charging station offers many benefits that streamline the charging process. By utilizing a license plate recognition system, the smart contract can transition more easily from vehicle identification to payment processing. This not only simplifies the user experience but also enhances security. The camera's input, the license plate number, is a simple string parameter that is easily transmitted through a wired connection. This method removes the need for implementing complex cryptographic operations within the smart contract itself, which are resource-intensive and can introduce additional points of failure. The simplicity of this setup reduces the attack surface for potential security breaches and makes the overall system more robust.

Moreover, this approach allows for the decentralization of certain aspects of the charging process. By enabling the charging station to perform some of its operations offline, we can evade the risks associated with network dependencies. For instance, in the event of a network outage, the charging station can continue to operate effectively, recognizing vehicles and processing transactions with the data stored locally. Once connectivity is restored, these transactions can be synchronized with the blockchain, ensuring that all data remains accurate and up to date without disrupting the charging service.

The hardware implementation of an Arduino or similar microcontroller adds a layer of physical security and operational reliability to the system. Microcontrollers are well-suited to real-time tasks such as license plate recognition and display control. They offer a low-cost, low-power solution that can run continuously, with minimal maintenance. This ensures that the charging station can operate independently of more complex computer systems, which may require regular updates and are more susceptible to cyber-attacks.

In terms of customer engagement, the smart contract can now handle other tasks for lower transaction costs, such as awarding points for using the charging service, not only promoting customer loyalty but also encouraging sustainable behavior. Users become part of a rewarding ecosystem that supports the adoption of electric vehicles, contributing to environmental sustainability. The smart contract's ability to calculate reward points based on actual usage introduces a gamification element to the charging process, making it more engaging for users.

Furthermore, the backend server's role in setting tariffs and reward rates ensures that the charging station remains compliant with local regulations and market conditions. This adaptability is crucial for businesses operating in multiple jurisdictions, enabling them to tailor their offerings to the specific needs and regulations of each location. The smart contract's ability to handle these variables in real-time and adjust the charging and rewards accordingly provides a flexible and responsive system that can quickly adapt to changes in market dynamics or regulatory requirements.

By enhancing the customer experience and operational efficiency, this integrated smart contract and hardware solution paves the way for a new standard in EV charging stations. It exemplifies how the convergence of blockchain technology with practical hardware can create innovative solutions that benefit businesses and consumers alike.

IV. Smart Contract for Offline Charging System

When a blockchain transaction is scheduled or carried offline, smart contracts can handle more complex functions without compromising much of their deployment cost.

Figure 1 shows a decision tree that represents the logic steps that the system will follow to be able to offer the client an offline payment option.

Initially, the camera system attempts to read the license plate of the vehicle. If the license plate is read correctly and matches a known license, the screen displays the user's profile options, including any accumulated reward points. This is managed by the identification function within the smart contract, which not only checks the registration status of the user but also handles new user registration if necessary.

In cases where the license plate cannot be read correctly or is unknown, the system provides the user with the option to retry reading the plate or request manual input by an employee, thereby ensuring that there are multiple pathways to user identification and that the process does not become a bottleneck.

Once the user is identified, they are prompted to choose the duration of the charging session. This user input triggers the *chooseTimespanAndCalculatePrice* function within the smart contract, which calculates the cost based on the selected timespan. The user is then asked to confirm the price, ensuring transparency and consent before proceeding.

For authentication and payment, the user has the choice of using NFC or a QR Code. This allows for flexibility in payment methods, catering to user preferences and the availability of technology. Upon successful authentication, the system performs a check user balance function to ensure that the user has sufficient funds to cover the charging cost.

If the balance is sufficient, the *pay* function is executed, and the user proceeds to pay for the charging session. In the event of insufficient funds, the user would need to address the balance issue before proceeding.

Additionally, the smart contract is designed to be responsive to electrical load management and market demand. It does not become overburdened by off-chain vehicle authentication and maintains rapid processing speeds. A tiered pricing model is integrated within the smart contract, which can adjust prices during peak and off-peak hours. This model incentivizes users to charge during less busy periods, contributing to a more balanced and efficient grid.

The smart contract also includes a *calculateRewards* function, which operates after the charging session to update the user's reward points based on the duration and timing of the charge. This encourages repeat usage and fosters customer loyalty.

A system like this is dependent on the cooperation of three components: camera(s) programmed in a low level language like C (the most common for embedded systems), microcontroller(s) for the display of QR codes, reward points and other functionalities that are part of the user-machine interaction, and lastly a smart contract that will handle the interaction with blockchain. For the model presented here, we created and tested an Ethereum smart contract prototype written in the Solidity language, that interact with the other two components through function parameters given as inputs from direct cable connection.

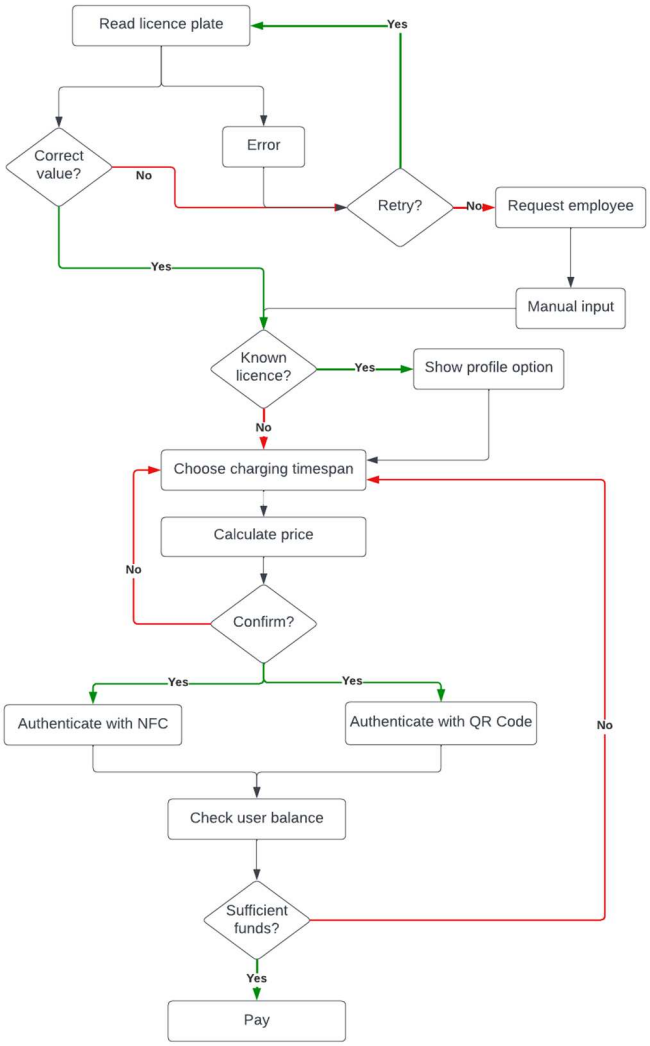

Fig. 1. Flow of electric vehicle identification, charging and payment model using license plate - based identification and NFC/SMS payment

V. RISK MANAGEMENT

Despite these advantages, one must carefully consider the challenges posed by offline payments, particularly concerning dispute resolution and payment verification. Here are some structured solutions to these challenges:

1. **Manual Verification Process**: In instances where offline payments are made, a reliable manual verification process is necessary. This could involve dedicated personnel who confirm the validity of payment receipts against the smart contract's records, ensuring that every transaction is accounted for and appropriately updated within the system.
2. **Prompt Transaction Confirmation**: Following the manual verification, the smart contract should be promptly updated to reflect the new balance. This could mean generating a physical confirmation document or updating the contract's

ledger on the blockchain. Although this may incur a minimal fee, it's a trade-off for the assurance and convenience provided to both the user and the operator.

3. **Risk Mitigation Policies**: Offline payments do carry a heightened risk, such as the chance of a payment failure due to insufficient funds. To address this, it is vital to establish transparent policies. For example, if the charging station has internet connectivity through a wired connection to an external computer that has internet access, it could check the user's balance, beforehand.

4. **Building Trust and Ensuring Transparency**: Notably, offline payments can engender a higher degree of trust among some users due to their resemblance to traditional, non-digital payment methods, which are perceived as less susceptible to cyber threats. This trust is founded on the conventional reliability of tangible payment methods like cash or checks.

5. **Seamless Technology Integration**: Even while operating offline, the system can incorporate hardware devices capable of documenting transactions. These devices can store transaction data temporarily and, once connectivity is restored, transmit the data to the contract owner for confirmation and reconciliation.

6. **Personal Data Protection**: A special attention must be paid to the protection of personal data collected and processed during the processes and stored in the system, according to positive legislation (e.g. GDPR [15]).

While offline payments may not provide the immediate convenience and automation of their online counterparts, with strategic management and the implementation of protocols, they can offer a secure and efficient alternative. The key lies in understanding the intrinsic risks and establishing a clear framework to handle them, thereby ensuring a reliable and user-friendly service.

Emphasizing the importance of user feedback is essential for enhancing the suggested framework and continuously improving the electric vehicle (EV) charging model. Incorporating a feedback loop within the system enhances its flexibility and increases user satisfaction. The suggested model may adapt, and change based on input from EV owners to better meet the changing requirements and preferences of its users. This method guarantees that the charging infrastructure stays both technologically modern and user-centric, adapting to real-world applications and user experiences. This little but significant feature demonstrates the model's commitment to continuous improvement and strong customer interaction, reinforcing its unique approach to the changing difficulties in the EV charging industry.

VI. CONCLUSION

In this paper, we propose a model for offline payments in electric vehicle (EV) charging systems, using license plate-based authentication with SMS-based transactions or NFC communication for payments, leveraging blockchain technology. The aim is to address issues like the lack of trust among EV charging stakeholders and the inconvenience of current payment methods. By using blockchain technology, the model seeks to streamline the authentication process, manage charging tariffs, calculate rewards, and process secure payments without the need for a continuous internet connection. This would potentially increase efficiency and trust in EV charging systems, addressing the problems identified in previous studies and providing a more user-friendly approach to EV charging.

The smart contract is designed to facilitate the outlined EV charging model on a blockchain. It includes structures to handle user registration via license plate numbers and maintains a balance and reward points for each user. The contract functions allow for the calculation of charging costs based on selected timespans and the processing of payments through SMS or NFC methods. Additionally, it includes the capability to calculate and allocate reward points after charging sessions. The contract is intended to work with external systems such as oracles for real-world data integration and would interact with physical charging stations. It aims to automate the EV charging process, making it secure and efficient while using blockchain technology to maintain an immutable record of transactions and reward points accumulation.

REFERENCES

[1] U.S. Bank (2022) U.S. bank expands card rewards to put EV charging transactions on par with gas, U.S. Bank. Available at: https://www.usbank.com/about-us-bank/company-blog/article-library/us-bank-expands-card-rewards-to-put-ev-charging-transactions-on-par-with-gas.html (Accessed: 28 November 2023).

[2] Rathner, S. (2023) Credit cards charge ahead with rewards for Driving Electric, NerdWallet. Available at: https://www.nerdwallet.com/article/credit-cards/why-credit-cards-are-charging-ahead-with-ev-related-rewards (Accessed: 28 November 2023).

[3] Shepard P. (2019) Using Blockchain to Drive Electric-Vehicle Charging Infrastructure, EE Power. Available at: https://eepower.com/news/using-blockchain-to-drive-electric-vehicle-charging-infrastructure/#

[4] Afif Monrat, A., Schelen, O. and Andersson, K. (2020) 'Blockchain Mobility Solution for charging transactions of electrical vehicles', 2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC) [Preprint]. doi:10.1109/ucc48980.2020.00055.

[5] Kim, M. et al. (2019) 'A secure charging system for electric vehicles based on Blockchain', Sensors, 19(13), p. 3028. doi:10.3390/s19133028.

[6] Guo, S. et al. (2022a) 'An electric vehicle charging transaction model based on Blockchain', 2022 International Conference on Blockchain Technology and Information Security (ICBCTIS) [Preprint]. doi:10.1109/icbctis55569.2022.00042.

[7] Okwuibe, G.C. et al. (2021) 'A blockchain based electric vehicle smart charging system with flexibility', IFAC-PapersOnLine, 53(2), pp. 13557–13561. doi:10.1016/j.ifacol.2020.12.800.

[8] Khoumsi, A. (2021) 'An efficient blockchain-based Electric Vehicle Charging Management System', 2021 IEEE Symposium on Computers and Communications (ISCC) [Preprint]. doi:10.1109/iscc53001.2021.9631412.

[9] Joyce Jacob, J. et al. (2023) 'Electric Vehicle Wireless charging using RFID', E3S Web of Conferences, 399, p. 01010. doi:10.1051/e3sconf/202339901010.

[10] Arakelyan, A. (2023) Fully Automated Charging of Electric Vehicles, Merlin. thesis. Available at: https://www.merlin.uzh.ch/contributionDocument/download/15650 (Accessed: 28 November 2023).

[11] Nowak, M. (2023) Learn all about NFC tags - A beginner's guide, Nomtek. Available at: https://www.nomtek.com/blog/what-are-nfc-tags (Accessed: 28 November 2023).

[12] Blockchain - Full offline mode (no date) Samourai Wallet. Available at: https://samouraiwallet.com/offline (Accessed: 28 November 2023).

[13] Brittany (2024) *Using mew offline | myetherwallet help center*, *MEW*. Available at: https://help.myetherwallet.com/en/articles/6512619-using-mew-offline.

[14] Cryptocurrencies and Blockchain Technology Applications by Gulshan Shrivastava (editor), Dac-Nhuong Le (editor), Kavita Sharma (editor), pp. 30-37. Available at: ttps://www.wiley.com/en-fr/Cryptocurrencies+and+Blockchain+Technology+Applications-p-9781119621164

[15] Intersoft Consulting (2021) Personal data, General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/issues/personal-data/.