

A Framework Solution for Vehicle Theft Detection by Integrating NFC With a Blockchain-Based System

Elva Leka^{1,2}, Luis Lamani¹, Klajdi Hamzallari¹

¹ Polytechnic University of Tirana, Tirane, Albania

² Albanian University, Department of Engineering, Faculty of Applied and Economic Sciences, Tirane, Albania

Abstract – Vehicle theft is a widespread and costly problem with thousands of cars stolen annually, impacting privacy, the economy, and security. Conventional database systems have proven unreliable, enabling a thriving market for stolen vehicles. In response, our study presents an innovative solution, leveraging the security of blockchain technology. By utilizing the Ethereum Virtual Machine (EVM) and Smart Contracts, our system is designed to thwart attacks, including Distributed Denial of Services (DDoS) attacks. Notably, Near Field Communication (NFC) enables the secure transmission of sensitive data for verification. Our research aims to evaluate the real-world impact of this technology, considering factors such as improvements in data security and the efficiency of the reporting process. One of the most notable outcomes of our proposal is the substantial reduction in reporting time for car theft. While conventional reporting typically takes several hours, our system streamlines the process to less than 1 minute. This innovation offers significant benefits to vehicle owners, law enforcement agencies, and the broader community.

Keywords – Blockchain, smart contract, NFC, vehicle theft, IPFS.

DOI: 10.18421/TEM124-16

<https://doi.org/10.18421/TEM124-16>

Corresponding author: Elva Leka,
Polytechnic University of Tirana, Albania
Albanian University, Tirane, Albania


Email: elva.leka@fgjm.edu.al

Received: 29 July 2023.

Revised: 09 October 2023

Accepted: 14 October 2023.

Published: 27 November 2023.

 © 2023 Elva Leka, Luis Lamani & Klajdi Hamzallari; published by UIKTEN. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.

The article is published with Open Access at <https://www.temjournal.com/>

1. Introduction

The significance of vehicles in our lives is undeniable as nearly 91.5% of American households possess at least one. Despite this, vehicle theft continues to be a significant concern. On average 4766.08 vehicles out of every 100,000 were reported as stolen in 2021 [1]. Most of the time stolen cars are either disassembled for their parts or swiftly sold locally or overseas for nefarious activities or joy trips. The problem has worsened because of unethical techniques to break into cars despite advancement in car security systems. The effects are notably more significant in third-world or developing countries where auto theft is prevalent.

Car owners must communicate with the police immediately upon discovering that their vehicle has been stolen. The chances of recovering the car greatly depend on the report's timing. Any delay in reporting the theft can reduce the likelihood of a successful retrieval. This article aims to address the issue of the time gap between reporting a stolen car and filing an official report. It suggests a workaround that utilizes blockchain technology [2].

According to this research, utilizing blockchain technology can efficiently and securely address the issue of unreported stolen vehicles [3]. Blockchain technology's immutability and security features guarantee data integrity [4]. This innovative method intends to revolutionize the reporting of car theft and enhance the chances of retrieval by enabling a fast, transparent, and dependable exchange of information.

In the following sections, we will examine how blockchain can alter the auto theft reporting scenario, focusing on its secure and real-time nature. We aim to illustrate the potential of blockchain technology as a game changer in preventing vehicle theft, minimizing the time lag between theft occurrence and reporting, and boosting the overall efficiency of law enforcement activities through the process of our inquiry.

Section 2 provides an overview of the background and related work. Section 3 describes the technologies used in the implementation of this framework. Section 4 introduces the concept of NFC and its integration with blockchain in our solution. In Section 5, we present the implementation details. Finally, we conclude in Section 6.

2. Related work

The main focus of this paper is on the advantages of blockchain technology, such as its resilience against DDoS attacks, data immutability, and decentralized architecture. Unlike traditional databases, blockchain operates on a decentralized network of nodes, assuring data integrity and resistance to tampering. A distributed ledger implementation enables real-time updates, increased transparency, and enhanced security measures, making it an ideal alternative for vehicle theft prevention systems.

By exploring relevant works [5], [6], [7], [8], [9], [10] and case studies, we highlight the potential of blockchain in revolutionizing vehicle security and theft prevention.

A system that minimizes vehicle theft, by notifying the vehicle owner with an alert message as soon as it is stolen or moved without his knowledge is proposed in study [6]. By integrating the Global System for Mobile Communication (GSM) technology and ESP32 Camera module, the system also helps to identify car's location and thief's picture.

The benefits and challenges of creating the Internet of Vehicles (IoV) have been introduced by Peng *et al.* [8]. They have also analyzed the potential advantages that blockchain technology could offer to Internet of Things (IoT).

A platform based on blockchain technology that aids in identifying, authenticating, and monitoring vehicles that may be involved in criminal activities is discussed in article [9]. This platform utilizes a shared blockchain database across devices to verify if a car has been stolen and employs cameras to track suspicious vehicles.

In their research [10], the authors examined the integration of Intelligent Transportation System (ITS) into smart cities and the challenges that arise in terms of trust, security, and vulnerability to vehicle authentication and validation due to the centralized system. They first identified various methods proposed to address these challenges using blockchain technology. Then, they presented a blockchain solution that focuses on ensuring the validity of Personal Identification Information (PII) to enhance the security of vehicle authentication.

Blockchain technology has emerged as a powerful tool for enhancing vehicle security due to its unique features. Unlike traditional databases, blockchain operates on a decentralized network of nodes, ensuring data integrity and resistance against tampering [11]. Implementing a distributed ledger allows for real-time updates, improved transparency, and enhanced security measures, making it an ideal solution for vehicle theft prevention systems.

Real-world Examples of Blockchain in Vehicle Security:

Several notable examples demonstrate the successful implementation of blockchain in vehicle security. For instance, the MOBI (Mobility Open Blockchain Initiative) [12] consortium explores the use of blockchain for tracking vehicle ownership, maintenance history, and accident records. Using a blockchain-based registry, relevant stakeholders can securely store and access information, reducing fraud, and ensuring transparency in the used vehicle market.

Another example is the partnership between BMW and VeChain [13], [14], where blockchain technology is employed to combat odometer fraud. Recording mileage data on the blockchain makes it immutable and tamper-proof, preventing fraudulent practices and providing potential buyers with accurate vehicle information.

In addition, the Car eWallet project [15], led by IOTA Foundation and partners including Jaguar and Land Rover aims to create a secure and decentralized payment system for various vehicle-related services. The project utilizes blockchain technology to ensure secure and transparent transactions between vehicles and service providers, enhancing overall security and efficiency.

3. Technologies

The primary focus will be utilizing decentralized technologies, which are more challenging to target and disable.

A. Blockchain

Blockchain technology is a recent innovation that has gained substantial traction in recent years. It is built upon foundational concepts established years ago and has experienced exponential growth. As its core, blockchain is a shared ledger, accessible to all network participants. Its internal mechanisms make it particularly suitable for safeguarding data against tampering and creating immutable records emphasizing decentralization. As a result, this technology introduces a new level of data integrity, surpassing that of alternative solutions.

The transaction structure of a block is presented in Figure 1.

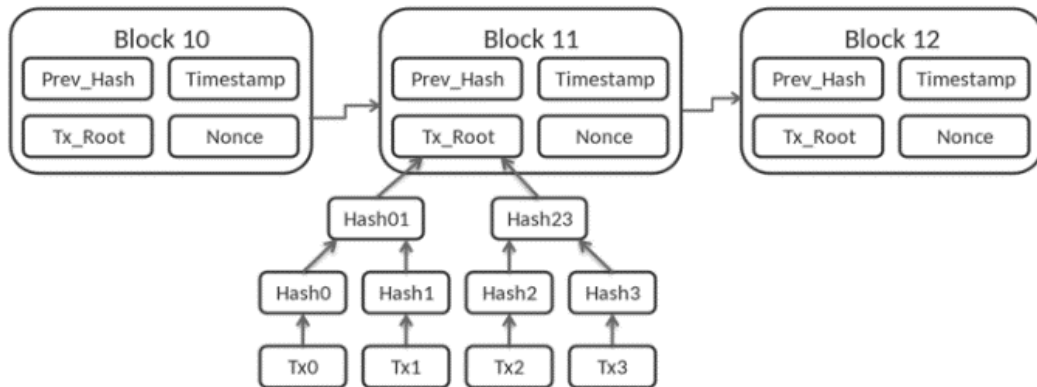


Figure 1. Transaction structure of a block

Despite its recent surge in publicity, blockchain technology is based on the fundamental principles of informatics and data structures. Essentially, blockchain is made up of a series of interconnected records organized into blocks. These blocks are connected to both the preceding and succeeding blocks through a sequence of cryptographic processes, and each block has a distinct identity that includes its hash, confirmation time, and data [16]. It is important to note that combining the previous block's hash with its content determines each block's hash. This method guarantees that any minor modification made to any prior block will affect the entire chain, invalidating all subsequent blocks. This interconnection of blocks through hash references creates a blockchain's unique chain structure.

B. EVM

The Ethereum Virtual Machine (EVM) [17] is responsible for executing instructions within the network, similar to the processors in our computers and smartphones. It can be connected to the processors found in our computers or smartphones that carry out user-initiated commands and store them within the network. However, the EVM operates distributed by dispersing operations, instructions, and data to all machines or nodes within the network. This creates a cohesive environment by unifying the processing, instruction execution, and data storage across all nodes [18].

Figure 2 presents the EVM structure. When executing instructions on the EVM, the concept of “gas” is employed as a measure of execution. Each transaction has a gas limit, known as *gasLimit*, which the initiator defines. This limit sets the maximum amount of gas that can be expended for executing a specific set of instructions [19].

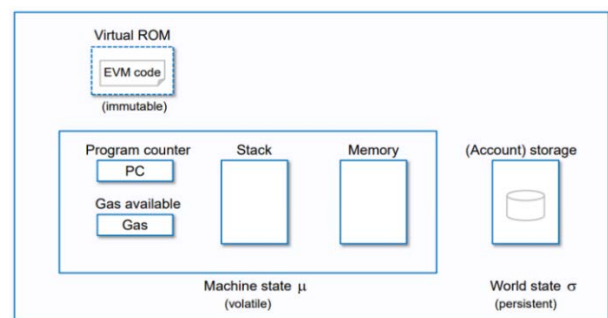


Figure 2. The EVM structure

C. Smart Contracts

Solidity is a (OOP) high-level object-oriented programming language in use since 2014. It is comparable to well-known programming languages such as Java C++, JavaScript, and Python. Primarily, Solidity serves the purpose of crafting smart contracts and undergoes compilation into bytecode. Subsequently, this bytecode is executed directly within the Ethereum Virtual Machine (EVM) [20].

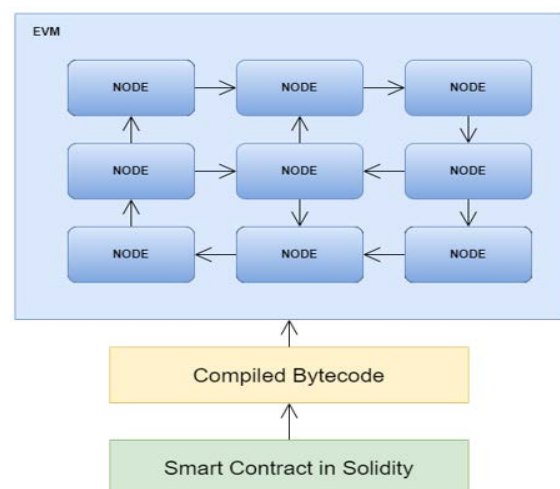


Figure 3. Deploying a smart contract in EVM

Automating instructions becomes possible through the programming and deployment of smart contracts, eliminating the need for manual intervention at a later stage [21]. In the case of vehicle development and real-time verification within the blockchain network, these smart contracts serve as the key facilitators. While blockchain is commonly regarded as a shared database, it lacks a predefined database structure. To address this, smart contracts are utilized to define the required data structure, tailored to record and keep relevant vehicle features. Consequently, this smart contract takes charge of managing the deployment and verification of vehicles within the system.

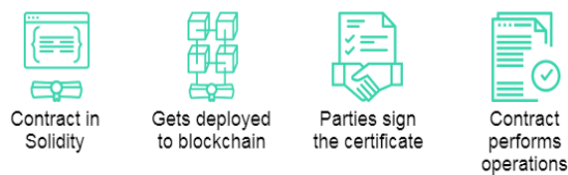


Figure 4. Smart contract life cycle

D. IPFS

IPFS, which stands for InterPlanetary File System, is a decentralized approach of storing large-scale data [22]. It operates on a peer-to-peer protocol, allowing for distributed storage and retrieval across a network. Content addressing is used to locate files on IPFS, similar to traditional torrent protocols [23], [24]. The data is distributed among network peers and can be accessed using a distributed hash table (DHT) [25]. As presented in Figure 5, directed acyclic graphs (DAG) [26], distributed hash tables (DHT) [25], and content addressing [22] are the three main pillars around which IPFS is based.

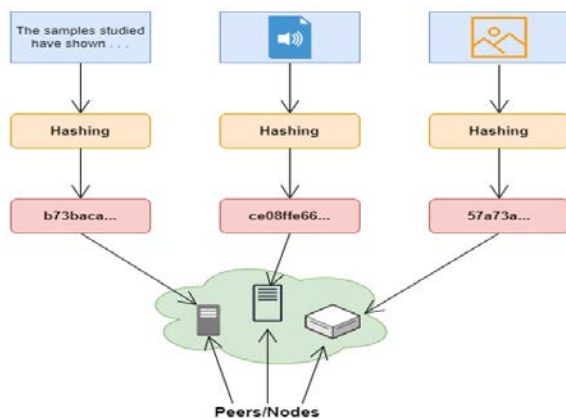


Figure 5. Uploading a file to IPFS

4. NFC tags

This research provides a unique concept for utilizing Near Field Communication (NFC) technology [16] to improve vehicle theft verification's user interface and effectiveness.

Some researchers have also proposed to integrate blockchain and NFC. In their paper [27], authors have proposed to use blockchain and NFC tag to track the history of products. NFC tag would help the owner of the product to connect with it and be used to sign the blockchain transactions. Through the architecture they propose they can achieve holistic tracking of products.

Meanwhile, authors in their paper [28] have proposed integrating blockchain technology and NFC to mitigate the issue of fake COVID-19's vaccination certificates.

Usually, users have to manually enter codes or search online to find out if a vehicle has been stolen. However, our proposed solution uses NFC technology to simplify and streamline the process, making it faster and more efficient. This will eliminate the need for time-consuming and tedious steps.

NFC technology allows for seamless communication between devices at proximity. By integrating the NFC tag discreetly within the vehicle, users can simply scan the tag using a mobile application specifically designed for this purpose. The mobile application instantly retrieves and displays the relevant information regarding the vehicle's theft status, eliminating the need for manual code entry or online queries. This innovative approach saves time and effort and enhances user convenience and engagement.

The NFC tag embedded within the vehicle serves as a unique identifier, securely linked to the vehicle's theft status in the blockchain network. When the user scans the NFC tag, the mobile application initiates a secure and encrypted communication with the blockchain, retrieving the real-time theft status information associated with that specific vehicle. The mobile application then promptly displays the results, indicating whether the vehicle has been reported stolen or not.

This NFC-based solution offers several notable advantages. Firstly, it significantly simplifies the verification process, allowing users to effortlessly check the theft status of their vehicles with just a quick scan. Additionally, NFC technology ensures a reliable and secure connection between the mobile application and the vehicle's embedded NFC tag [29], minimizing the risk of unauthorized access or tampering. Moreover, the real-time retrieval of theft status information from the blockchain network guarantees up-to-date and accurate results.

We aim to make customers happier, reduce the amount of human labor required, and speed up the reporting and identification of stolen cars by integrating NFC technology into the vehicle theft verification process.

By using a user-friendly mobile application that seamlessly integrates NFC technology, we provide a simple and effective solution for those concerned about the security of their vehicles. The revolutionary approach will completely change the way vehicle theft verification is carried out, ultimately helping to recover and prevent stolen cars.

5. Implementation

In this section firstly we will describe the proposed system's architecture, and then present the pseudocode of smart contract on which the system's main functions will be implemented.

A. System architecture design

Figure 6 presents the architecture of the system and the flow of the activities of verifying a vehicle process.

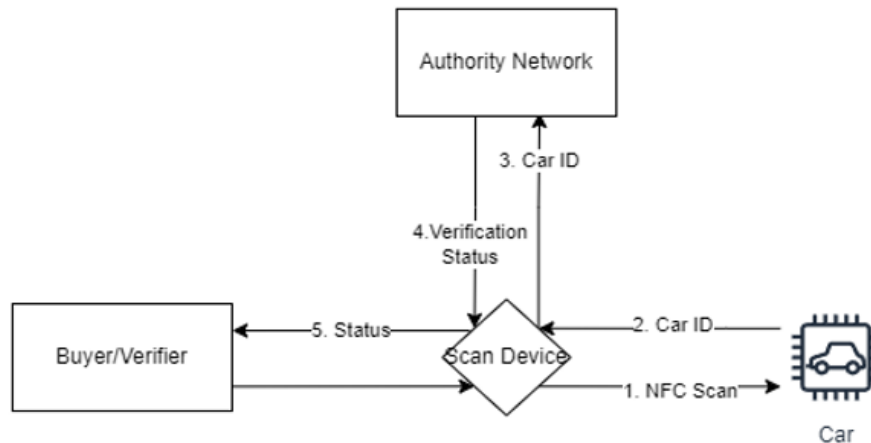


Figure 6. System architecture design

Once a vehicle is registered, the system records vital information including: (1) VIN (Vehicle Identification Number); (2) Model; (3) Make; (4) Color; (5) License Plate; (6) Owner name; (7) Image of the vehicle (if provided).

This entry can be initiated by the vehicle's first owner or updated by authorized entities, such as authorities or subsequent owners.

However, the process requires a specialized private key, accessible only to the vehicle owner. The system verifies if the private key corresponds to the vehicle owner or authorized parties. If the verification fails, the operation is aborted. The data is transmitted to the blockchain on successful verification, while the vehicle's photo is uploaded to the IPFS network. Figure 7 presents a simplified overview of modifying vehicle information.

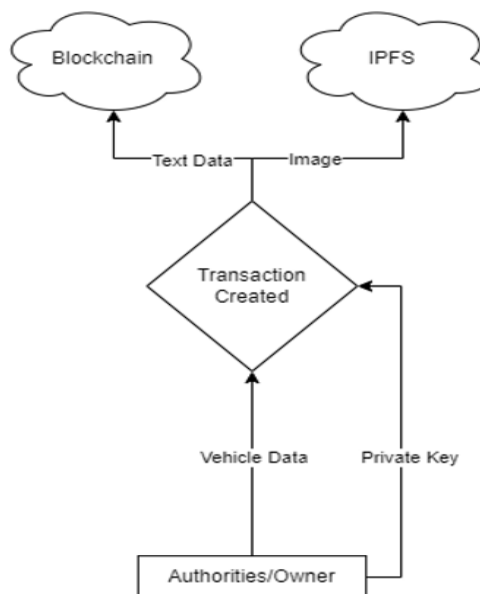


Figure 7. Simplified overview of modifying vehicles information

Meanwhile, Figure 8 presents the process of marking a vehicle as stolen.

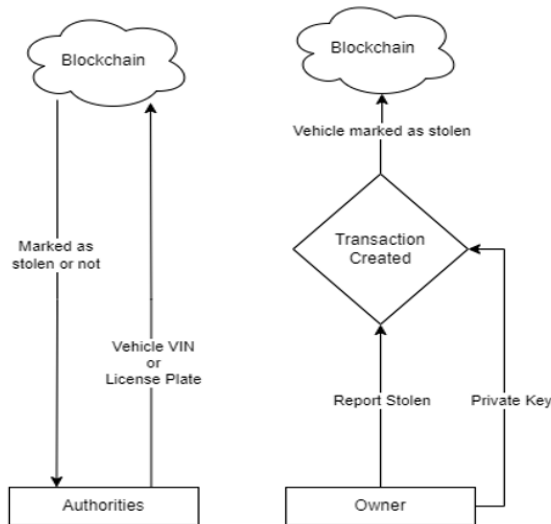


Figure 8. The process of marking a vehicle as stolen

Users can utilize the vehicle’s VIN and license plate to determine whether a car has been reported stolen. By submitting a request to the blockchain network, users receive a response containing a status code indicating the vehicle’s status. Additionally, the request includes information about the vehicle’s last known location, which can be manually entered annually or automatically obtained from GPS data.

Marking a vehicle as stolen requires a transaction, also known as confirmation, from either the vehicle owner or authorized authorities with appropriate access. The owner initiates the transaction by providing the vehicle’s VIN and/or license plate number. Subsequently, the owner enters their private key, which the network utilizes to verify their identity on the network. The network then confirms that the user is the vehicle’s owner before moving forward with the appropriate actions.

If a car is reported as stolen, it is placed at the top of the list of local stolen vehicles. Nearby authorities can visually compare incoming traffic to the car’s description, and if there is a match, they can investigate further by entering the license plate into the system. This simple process eliminates the need to call the authorities and provide an official statement. Additionally, the same process can be used to check vehicles sent abroad, and if a stolen car is found, authorities will be notified.

The network connection is established through everyday devices like computers and phones, enhancing the accessibility of the system. This simplified procedure drastically reduces the time needed to check and report stolen cars, which is essential in determining the likelihood of successfully recovering the vehicle.

B. The pseudocode of the smart contract

In Figure 9, the pseudocode of the smart contract we will develop for our proposed system is presented.

```
//Smart Contract
Contract CarStatus:
struct Car:
    address owner;
    string make;
    string model;
    bool isStolen;

uint256 carCount;

function registerCar(string make, string model):
    carCount+=1;
    cars[carCount] = Car(msg.sender, make, model, false)

function getCarStatus(uint256 carId) returns bool:
    require carId > 0 and carId <= carCount, "Invalid car ID"
    return cars[carId].isStolen;

function setCarStatus(uint256 carId, bool isStolen):
    require carId > 0 and carId <= carCount, "Invalid car ID"
    Require cars[carId].owner == msg.sender, "Only car owner can update status";
    cars[carId].isStolen = isStolen;
```

Figure 9. The pseudocode of ‘CarStatus’ smart contract

The provided code is a simplified implementation of a Solidity smart contract named *CarStatus*, related to the abstract discussing vehicle theft prevention using blockchain technology.

- *Struct Car*: this is a data structure defining the attributes of a car, including the owner, make, model (car model & VIN), and *isStolen*.
- *Function registerCar()*: This function allows authorities or car sellers to register vehicles on the blockchain. When called, it increments the *carCount*, creates a new *Car* instance with the provided make, model, and sets the ‘*isStolen*’ flag to false, indicating that the car is not stolen.
- *Function getCarStatus()*: This function allows everyone to query the status of a car by providing its *carID* as an argument. It checks if the *carId* is valid and then it returns the ‘*isStolen*’ status of that particular car.
- *Function setCarStatus()*: This function enables the car owner to update the ‘*isStolen*’ status of their car. It requires that the ‘*carID*’ is valid and that the caller (*msg.sender*) is the owner of the car or an authority. If both conditions are met, the function updates the ‘*isStolen*’ flag of the specified car to the value provided in the ‘*isStolen*’ argument.

Overall, this smart contract provides a basic framework for registering car information, checking the status of a car, and allowing appropriate actors to mark vehicles as stolen on the blockchain. In a complete implementation, additional features like access control, event handling, and more secure mechanisms would be required to ensure the robustness of the system.

6. Conclusion

A decentralized blockchain-based system paired with Near Field Communication (NFC) technology integration offers a convincing answer to the problem of vehicle theft. The system's utilization of blockchain technology provides a robust and secure platform, while NFC enhances user convenience and accessibility.

With blockchain technology, this system now boasts enhanced security features, that significantly reduce the risk of DDoS attacks. Moreover, the integrity of stored data is effectively maintained. Due to the blockchain's decentralized structure, all users can still access the system regardless of their physical location or infrastructure capabilities.

Additionally, integrating NFC technology streamlines the user experience by enabling seamless communication between vehicles and mobile applications. Users can simply scan NFC tags hidden within the car to instantly retrieve information on its theft status. This user-friendly approach enhances adoption rates and empowers individuals to actively participate in preventing vehicle theft.

In summary, the combined strength of blockchain technology and NFC integration creates a comprehensive user-centric solution for vehicle theft prevention. By combining the advantages of both technologies, we can create a straightforward and reliable system that individuals from various backgrounds can easily use. This novel strategy represents a significant development in the fight against auto theft and enhances general security in the automotive sector. Furthermore, we believe that our study contributions bring advancements in adapting blockchain technology in citizens' services, by improving the time, cost, security, and simplification of those services to the citizens.

References:

- [1]. Brenckle, J., & Stroisch, C. (2023). *NICB Report Finds Vehicle Thefts Continue to Skyrocket in Many Areas of U.S.* National Insurance Crime Bureau. Retrieved from: <https://www.nicb.org/news/news-releases/nicb-report-finds-vehicle-thefts-continue-skyrocket-many-areas-us> [accessed: 17 June 2023]
- [2]. Leka, E., Selimi, B., & Lamani, L. (2019). Systematic Literature Review of Blockchain Applications: Smart Contracts. *2019 International Conference on Information Technologies (InfoTech)*, Varna, Bulgaria, 1-3. Doi: 10.1109/InfoTech.2019.8860872.
- [3]. Vergaray, A. D., Rosales, H. J. F., & Cordova, R. L. (2023). Blockchain technology aimed at solving Internet of Things Challenges: A Systematic Literature Review. *TEM Journal*, 12(2), 757-768. Doi: 10.18421/TEM122-20.
- [4]. Leka, E., & Selimi, B. (2021). Development and evaluation of blockchain based secure verification and validation of academic certificates. *Annals of Emerging Technologies in Computing*, 5(2), 22-36.
- [5]. Karthiga, M., Nandhini, S. S., Tharsanee, R. M., Nivaashini, M., & Soundariya, R. S. (2021). Blockchain for Automotive Security and Privacy with Related Use Cases. In *Transforming Cybersecurity Solutions Using Blockchain* (pp. 185-214). Singapore: Springer Singapore.
- [6]. Wong, B., & Kokko, H. (2005). Is science as global as we think? *Trends in ecology & evolution*, 20(9), 475-476.
- [7]. Jaathya, A., Reddy, A. L., Nikhitha, G., & Anusha, C. (2022). Implementation of vehicle theft detection and identification system. *International Research Journal of Engineering and Technology (IRJET)*, 9(7), 1009-1011.
- [8]. Das, D., Banerjee, S., & Biswas, U. (2020). A secure vehicle theft detection framework using Blockchain and smart contract. *Peer-to-Peer networking and Applications*, 14, 672-686. Doi: 10.1007/s12083-020-01022-0.
- [9]. Gao, J., Peng, C., Yoshinaga, T., Han, G., Guleng, S., & Wu, C. (2023). Blockchain-Enabled Internet of Vehicles Applications. *Electronics* 2023, 12(6), 1335-1397. Doi: 10.3390/electronics12061335.
- [10]. Farr, Z., Azab, M. & Samir, E. (2020). Blockchain-based cooperative autonomous detection of suspicious vehicles. *2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC, Canada, 2020, 188-192. Doi: 10.1109/IEMCON51383.2020.9284881.
- [11]. Das, D., Dasgupta, K., & Biswas, U. (2023). A secure blockchain-enabled vehicle identity management framework for intelligent transportation systems. *Computers and Electrical Engineering*, 105, 108535. Doi: 10.1016/j.compeleceng.2022.108535.

- [12]. Ogrutan, P. L. (2020). An analysis on the opportunity of introducing blockchain technology in education – A case study. *TEM Journal*, 9(3), 971-976. Doi: 10.18421/TEM93-19.
- [13]. EUBlockchain Observatory and Forum. (n.d.). *Blockchain applications in the automotive sector*. EUBlockchain Observatory and Forum. Retrieved from: https://www.eublockchainforum.eu/sites/default/files/reports/eubof_automotive_2022_FINAL.pdf [accessed: 23 June 2023]
- [14]. She, Z. (2022). VeChain: A renovation of supply chain management – A look into its organization, current activity, and prospect. *2022 International Conference on Educational Informatization, E-commerce and Information System*, Francis Academic Press, UK. 292-297. Doi: 10.25236/iceieis.2022.067.
- [15]. Ashraf, M., & Heavy, C. (2022). Overview of a Prototype for Application of Blockchain Supply chain for traceability using VeChain, IoT, Sigfox as LPWAN. *European Decision Sciences Institute – EDSI*, Dublin, Ireland, May 2022.
- [16]. Albert, F., & Klein, L. *Blockchain and distributed ledger technologies in automotive use cases. A SWOT analysis of technological potential and implications for future cars*. Tech.rep. Retrieved from: https://webarchiv.typo3.tum.de/BGU/mobil-vt/fileadmin/w00bqi/www/mobilTUM2019/Sessions/Posters/6105_abstract.pdf [accessed: 05 July 2023].
- [17]. Ma, F., Ren, M., Fu, Y., Wang, M., Li, H., Song, H., & Jiang, Y. (2021). Security reinforcement for Ethereum virtual machine. *Information Processing & Management*, 58(4), 102565.
- [18]. Coskun, V., Ozdenizci, B., & Ok, K. (2015). The Survey on Near Field Communication. *Sensors*, 15(6), 13348-13405. Doi: 10.3390/s150613348.
- [19]. Dannen, Ch. (2017). *Introducing Ethereum and Solidity. Foundation of Cryptocurrency and Blockchain Programming for Beginning*. Apress. Doi: 10.1007/978-1-4842-2535-6.
- [20]. Ethereum. (2023) *Gas*. Ethereum Developers. Retrieved from: <https://ethereum.org/en/developers/docs/gas/> [accessed: 27 June 2023].
- [21]. Gai, Y., Zhou, L., Qin, K., Song, D., & Gervais, A. (2023). Blockchain Large Language Models. *Cryptography and Security*. *arXiv:2304.12749*. Doi: 10.48550/arXiv.2304.1279.
- [22]. Ma, F., Fu, Y., Ren, M., Wang, M. (2019). EVM: From Offline Detection to Online Reinforcement for Ethereum Virtual Machine. *2019 IEEE 26th International Conference on Software Analysis, Evolution and Reengineering (SANER), Hangzhou, China, 2019*, 554-558. Doi: 10.1109/SANER.2019.8668038.
- [23]. Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System. *Networking and Internet Architecture*, *arXiv:1507.3561*. Doi: 10.48550/arXiv.1407.3561.
- [24]. Doan, T. V., Psaras, Y., Ott, J., & Bajpai, V. (2022). Towards Decentralised Cloud Storage with IPFS: Opportunities, Challenges, and Future Directions. *IEEE Computer Society*, *arXiv:2022.06315*. Doi: 10.48550/arXiv.2202.06315.
- [25]. Leka, E., Kordha, E., & Hamzallari, K. (2022). Towards an IPFS-Blockchain based Authentication/Management system of academic certification in Western Balkans. *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, Opatija, Croatia, 1448-1453. Doi: 10.23919/MIPRO55190.2022.9803625.
- [26]. Zeng, R., You, J., Li, Y., & Han, R. (2022). An ICN-Based IPFS High-Availability Architecture. *Future Internet* 2022, 14(5), 122. Doi: 10.3390/fi14050122.
- [27]. Huang, H.-S., Chang, T.-S., & Wu, J.-Y. (2022). A Secure File Sharing System Based on IPFS and Blockchain. *Cryptography and Security (cs.CR)*, *arXiv:2205.01728*. Doi: 10.48550/arXiv.2205.01728.
- [28]. Bohem, V., Kim, J., Hong, J. (2018). Holistic tracking of products on the Blockchain using NFC and verified users. In *Information Security Applications*, 184-195. Doi: 10.1007/978-3-319-93563-8_16.
- [29]. Ishengoma, F. (2021). NFC-Blockchain based COVID-19 immunity certificate: Proposed system and emerging issues. *Information Technology and Management Science*, 24, 26-32. Doi: 10.7250/itms-2021-0004.
- [30]. Ylinen, J., Koskela, M., Iso-Anttila, L., & Loula, P. (2009). Near Field Communication Network Services. In *2009 Third International Conference on Digital Society*, 89-93. Cancun, Mexico. Doi:10.1109/ICDS.2009.43.