Implementing Blockchain and Smart Encryption for Immutable Purchase and Generates Digital Ownership Certificates

ARSHDEEP SINGH SODHI, SANJANA DAS, SATHYAPRIYA L.
Department of Computing Technologies
SRM University, KTR
Chennai 603203, INDIA

Abstract: —Blockchain functions as a decentralized and distributed ledger technology, ensuring the secure recording and verification of transactions across a network of computers. It tackles trust, transparency, and resistance to tampering in conventional centralized systems by creating a clear and unalterable transaction record, eliminating the necessity for a central authority. Addressing trust-related challenges in transactions, Blockchain eliminates intermediaries, diminishes fraud risks through cryptographic security, and boosts transparency by establishing an immutable shared transaction history. The proposed system, built on a blockchain foundation, aims to securely and efficiently store purchase details by utilizing a duplicated and distributed digital ledger of transaction records across all participant computers in the network. Key features such as immutability, enhanced security through smart contracts and encryption, digital ownership certificates for authenticity verification, and a user-friendly search function contribute to the secure storage of purchase details. This innovative system extends the transformative impact of blockchain to the insurance industry, providing a decentralized alternative to counter centralization, inefficiency, and high costs. The result obtained enabling direct transactions between users and eliminating intermediaries, the system reduces frictional costs and enhances trust and transparency in insurance practices. This groundbreaking approach signifies a shift towards a more secure, efficient, and transparent future for both purchase record management and insurance processes, leveraging the full potential of blockchain technology.

Key-words: —blockchain, decentralized ledger, smart contracts, cryptographic security, transparent future.

Received: March 17, 2024. Revised: August 11, 2024. Accepted: September 15, 2024. Published: October 30, 2024.

1. Introduction

2.1 Blockchain Technology

Blockchain technology serves as a crucial element in the functionality of smart contracts. It operates as a distributed database structure that compiles information on past and future transactions within a network. Resembling a timestamped linked list, the blockchain continually expands with each added node, encompassing data related to network transactions and the cryptographically hashed address of the preceding block. This decentralized ledger system is replicated and shared among network participants, eliminating the need for a central server and allowing anonymous parties to engage in transparent, irreversible, and secure transactions and agreements. Smart contracts leverage blockchain for verification, validation, and the enforcement of agreed-upon terms between contracting parties. Each blockchain transaction includes sender and recipient addresses (commonly referred to as wallets) and transaction value/data. Notably, data stored in a blockchain is immutable, signifying that once stored, it remains unalterable. Network participants can view and engage in the verification and validation of transactions, bolstering network security. The illustration of the blockchain is depicted in Figure 1.

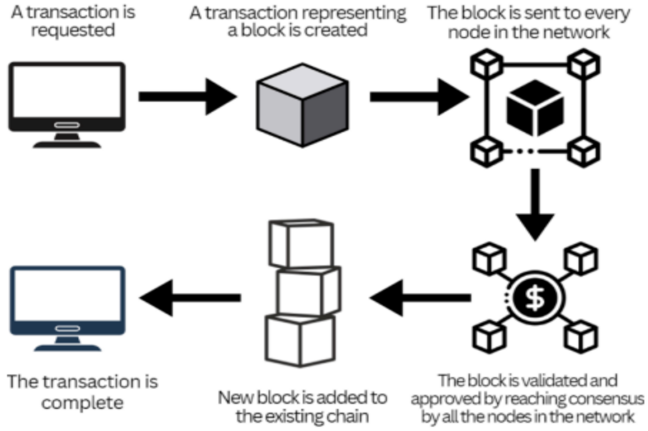

A transaction is requested
A transaction representing a block is created
The block is sent to every node in the network
The block is validated and approved by reaching consensus by all the nodes in the network
New block is added to the existing chain
The transaction is complete

Fig. 1. Structure and Functioning of the blockchain.

Mining involves actively participating in a blockchain system to verify transactions, and individuals undertaking this role are known as ”Miners.” A miner selects a fresh transaction from a list, integrates it into a new block, and engages in mathematical computations to solve functions, ultimately determining a unique ”nonce” value for the block. This entire process is designed to ensure that the new transaction is securely linked to a preceding transaction in the blockchain, preventing any malicious activities. Miners who successfully calculate a valid nonce for a blockchain are rewarded for their efforts. The newly formed block is then confirmed as a verified transaction and appended to the blockchain, prompting other miners to update their respective copies of the blockchain ledger.

2.2 Smart Contracts

A smart contract operates as an independent code that encapsulates the terms and conditions of a legal agreement within a computer program. This program functions autonomously, overseeing, executing, and enforcing the specified conditions. Stored on a blockchain, a decentralized and distributed ledger system, these contracts activate automatically when predefined conditions are met, potentially eliminating the need for a trusted third party. The parties involved in the agreement engage in negotiations to establish and agree upon the terms and conditions, which are then encoded. In essence, smart contracts act as a mechanism that distributes digital assets to the involved parties once a predetermined set of terms and conditions is fulfilled. These contracts self-execute on a secure network controlled entirely by computers. The foundational element enabling smart contract functionality is Blockchain technology, inheriting key characteristics from the blockchain, such as immutability and distribution. Immutability ensures that once a smart contract is created, it remains unalterable, resistant to tampering or interference. Distribution involves every member in the network validating the contract's outcome, preventing attackers from manipulating the release of funds. Participants can engage in smart contracts with transactions that are transparent, irreversible, and secure, thanks to the ledger system within the blockchain. Detailed mathematical terms are implemented using a programming language compatible with the blockchain platform to create the smart contract. Although various blockchains support smart contracts, Ethereum stands out as the most popular choice, with real implementation gaining prominence in 2016 through the Ethereum Blockchain, building upon the original concept introduced by Szabo.

Despite the increasing popularity of smart contracts, the development and execution of blockchain applications are still in their early stages, and the utilization of blockchain technology lags behind that of other technologies. The complexities surrounding the integration of blockchain and smart contracts often lead to confusion, and devising systems to replace traditional models poses significant challenges.

This research aims to propose a blockchain-centric solution for the shortcomings in current centralized insurance systems. The primary goal is to present a blueprint and a prototype implementation of a decentralized, community-driven insurance platform based on blockchain technology. The motivation behind this study lies in contributing to ongoing research on blockchain, specifically by exploring the secure adaptation of blockchain technology to replace intermediaries and advocating for a decentralized approach in the trustless insurance realm.

2. Literature Review

The B-FICA, a novel framework for Auto Insurance Claims and Adjudication built on Blockchain, introduces a private blockchain system that limits access to authorized parties on a need-to-know basis [1]. This innovative framework utilizes a partitioned ledger with a two-sided verification mechanism to monitor data and interactions within the network. Furthermore, it incorporates member consensus and multi-signed transactions to ensure transaction evidence, maintaining validity and reliability [1]. An evaluation of this framework indicates a significant reduction in processing time for auto insurance claims with minimal overhead. By integrating AES-256-CBC encryption, our project aims to enhance data protection, providing a more efficient defense against unauthorized access and data manipulation compared to existing methods. This encryption technology complements the unique features of B-FICA, ensuring robust security for sensitive information within the blockchain network.

Monireh Vahdati [2] introduces a Self-Organized Framework for Insurance, leveraging the Internet of Things (IoT) and Blockchain. This framework facilitates peer-to-peer communication among policyholders, police officers, and insurance agents. The proposed approach promotes the use of IoT processes, including sensors, to validate and assess claims. Additionally, the paper suggests the adoption of cryptocurrencies for quicker and transparent claim transactions, offering a novel payout method to policyholders. Mayank Raikwar presents a conceptualization blockchain-centric methodology for insurance transactions, providing a potential framework for adoption by insurance companies [3]. The prototype development involves the utilization of the Hyperledger smart contract platform, allowing an analysis of the performance and security implications associated with integrating blockchain into insurance processes. The research also explores the scalability of the network to assess the system's robustness, highlighting that the confirmation time is significantly influenced by the size of the network [3].Demir et al. propose a vehicle insurance management system that utilizes a tamper-free ledger of events. Blockchain technology is employed to create a tamper-free ledger, ensuring that once information is recorded, it cannot be altered or manipulated. This feature is crucial in the context of automobile insurance, where the accuracy and integrity of records play a pivotal role in resolving disputes and ensuring trust among stakeholders. The system advocates for the incorporation of blockchain technology to record transactions across all facets of automobile insurance. The blockchain ledger ensures the creation of tamper-proof records, offering transparency and serving as 'proof of insurance.' This verifiable documentation is valuable for stakeholders such as drivers, insurance companies, lawyers, and motor vehicle agencies in the event of a dispute [5].

Several studies have aimed to enhance transparency, secure communication, and maintain the integrity of shared data (6, 7). Ali Dorri and colleagues introduce an IoT integrated blockchain-based application aimed at ensuring automotive security and privacy (6). The paper focuses on leveraging blockchain technology to enhance security within the automobile insurance sector. The suggested architecture proposes the use of wireless software updates, changeable public keys, and dynamic premium pricing models integrated with a blockchain ledger. In a separate contribution, R. Roriz and J. L. Pereira (7) present a system designed for insurance companies to mitigate the risk of double-dipping insurance fraud, where a vehicle is insured in multiple policies. Their proposed solution involves implementing a blockchain-based system, where insurance companies act as nodes and have access to a blockchain ledger containing insurance policy information. This ensures that a specific vehicle receives only one insurance policy. Beyond the application of blockchain for data verification and integrity, the paper explores reputation management using blockchain technology. Yang and colleagues (8) introduce a reputation system for data credibility in their work. The proposed approach enables a network of vehicles to assess shared data based on reputation values.

3. Methodology

This section elaborates on the procedures employed for handling digital transactions using the Ethereum blockchain. We leverage the Metamask platform to ensure the permanence of all transactions, securely recording them in blocks to provide an additional layer of security. What distinguishes our project is the introduction of an insurance feature for users in the form of a digital ownership certificate. This certificate comprises a privacy key and public ID, granting users the ability to access transaction details at their convenience, even over extended periods. Our methodology involves the use of Solidity code in the Hardhat Ethereum development environment, incorporating state-of-the-art blockchain technology. Moreover, we enhance security by implementing the AES-256-CBC algorithm, known for its advanced and secure nature. This algorithm employs a 256-bit key, creating a vast and intricate combination that significantly diminishes the risk of unauthorized access. Additionally, our project prioritizes user experience by providing an intuitive and user-friendly interface.

3.1 Proposed Model

This study proposes a groundbreaking approach to managing purchase records, aiming to rectify inefficiencies and vulnerabilities inherent in current systems. By harnessing the capabilities of Ethereum blockchain technology, the suggested system guarantees a secure, transparent, and unchangeable repository for purchase information. The incorporation of smart contracts and AES-256-CBC encryption bolsters data security, protecting against unauthorized access and tampering. A notable innovation lies in the introduction of a ”digital ownership certificate,” which fosters trust in transactions by verifying authenticity. The system’s user-friendly search functionality facilitates effortless data retrieval based on various parameters.

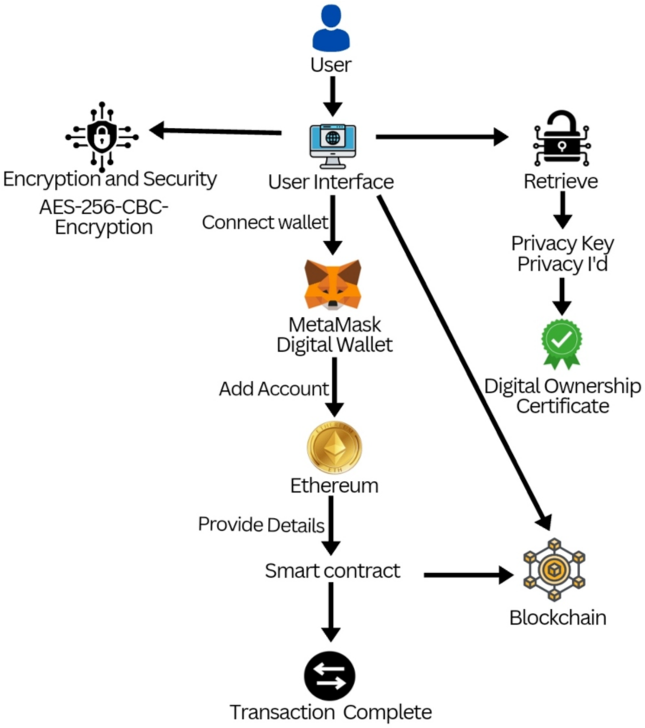


Fig. 2. System Design.

Expanding the application to the insurance sector, the decentralized model advocates for direct peer-to-peer transactions, reducing costs and augmenting transparency. Leveraging the distributed ledger technology of blockchain overcomes scalability challenges, ensuring efficient handling of extensive data volumes.The conventional method of documenting purchase information is frequently insecure, inefficient, and susceptible to manipulation. This research suggests the implementation of blockchain technology to achieve secure and unchangeable storage of purchase details. The proposed solution seeks to streamline data retrieval through an easily navigable search functionality, allowing users to filter information based on parameters such as image, purchaser name, date of purchase, or seller’s name.

To address concerns about security and efficiency in digital transactions, a blockchain-based application is recommended for the secure and unchangeable storage of purchase details. The introduction of a ”digital ownership certificate” adds an extra layer of verification for the authenticity of purchases. The proposed blockchain-centric platform not only revolutionizes the storage and retrieval of purchase data but also provides a scalable framework for transparency and efficiency across various industries.

The illustration of the insurance platform's design, utilizing blockchain and smart contracts, is depicted in Figure 3.

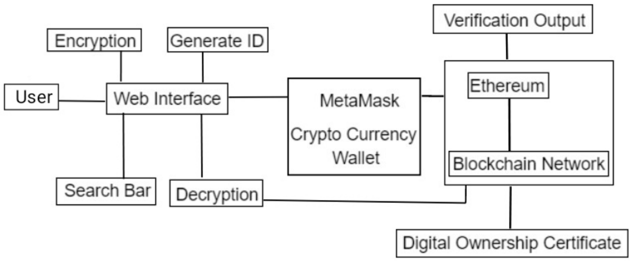


Fig. 3. Structure of decentralized insurance.

The features of the proposed system are described below

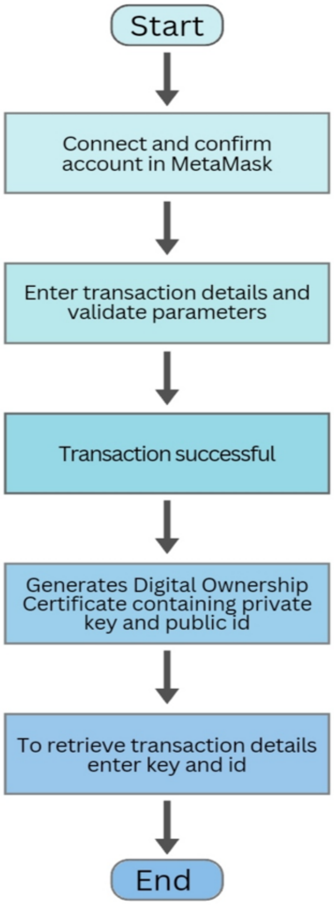

Start
Connect and confirm account in MetaMask
Enter transaction details and validate parameters
Transaction successful
Generates Digital Ownership Certificate containing private key and public id
To retrieve transaction details enter key and id
End

Fig. 4. Structure of decentralized insurance.

1. Connect and validate your account with MetaMask:
Objective: This stage entails the linking and authentication of your account through MetaMask.

Additional Details: It is crucial to incorporate the login component to enhance the user authentication process. MetaMask functions as a digital wallet for managing blockchain assets, and the account connection process involves securely confirming your identity.

2. Input transaction specifics and verify parameters:
Objective: This step requires entering transaction details and ensuring alignment with predefined criteria.

Additional Details: Emphasize accuracy and adherence to established criteria to accurately document and confirm transaction details for subsequent processing, minimizing the occurrence of errors or discrepancies.

3. Generate a Digital Ownership Certificate:
Objective: This procedure involves the creation of a Digital Ownership Certificate, comprising both a private key and a public ID.

Additional Details: The certificate serves as a secure means of establishing and verifying ownership in the digital realm. Private keys ensure secure access, while public IDs can be shared publicly to validate ownership.

4. Retrieve transaction details, input key and ID:
Objective: This stage involves accessing transaction details by providing the appropriate key and corresponding ID.

Additional Details: Input the key and ID associated with the transaction to retrieve its details. This process is vital for reviewing past transactions, ensuring transparency, and maintaining a comprehensive record of activities.

In summary, the suggested application utilizing blockchain technology provides a secure, streamlined, and transparent approach to store and access purchase information. Through the utilization of blockchain, smart contracts, and cutting-edge encryption, the system effectively tackles existing weaknesses found in conventional storage approaches. Incorporating digital ownership certificates and a user-friendly search feature further improves authenticity verification and information retrieval. The broader implications of this platform span across industries such as insurance, highlighting its capacity to enhance transparency and operational efficiency.

3.2 Technology Used

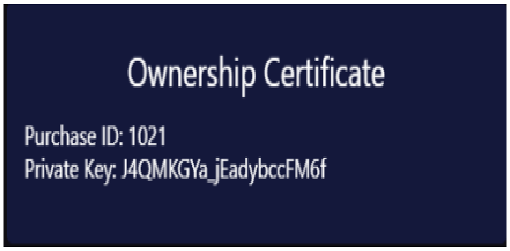
- Web 3.0 Blockchain Network: The term refers to the advanced internet infrastructure, commonly known as Web 3.0, which incorporates blockchain technology. The use of blockchain allows for decentralized and trustless interactions, reducing reliance on traditional centralized control and establishing trust through cryptographic principles.
- Impressive Design Linked to Metamask Pairing: The application's user interface boasts an attractive design seamlessly integrated with Metamask. Metamask, a cryptocurrency wallet, enhances the visual appeal of the interface while ensuring the security of user interactions with the blockchain through pairing.
- Engaging with Smart Contracts and Initiating Ethereum Transactions: Users can actively engage with and execute

smart contracts on the blockchain network using the application. Smart contracts, self-executing agreements with terms coded directly, provide users the ability to initiate transactions using Ethereum, a popular cryptocurrency operating on the blockchain.

- Implementing Solidity Code: The application employs Solidity, a programming language designed for creating smart contracts on blockchain platforms, especially Ethereum. This highlights that the application is developed using Solidity to define and deploy various blockchain-based functionalities.
- Integrating React.js Application with the Blockchain Network: The application utilizes React.js, a widely adopted JavaScript library, to construct the user interface. Known for creating dynamic and responsive user interfaces, React.js is linked to the blockchain network, enabling users to seamlessly interact with decentralized applications.
- VITE - Advanced Frontend Tooling: VITE serves as a contemporary frontend build tool, facilitating swift development, efficient bundling, and improved performance. Leveraging VITE accelerates the development process, enhancing overall efficiency and resulting in an improved user experience.
- Utilizing Tailwind CSS for Design: Tailwind CSS, a utility-first CSS framework, streamlines the styling process by providing pre-defined utility classes for efficient application design and styling. This strategic choice ensures a visually appealing and responsive design for the application.

4. Results

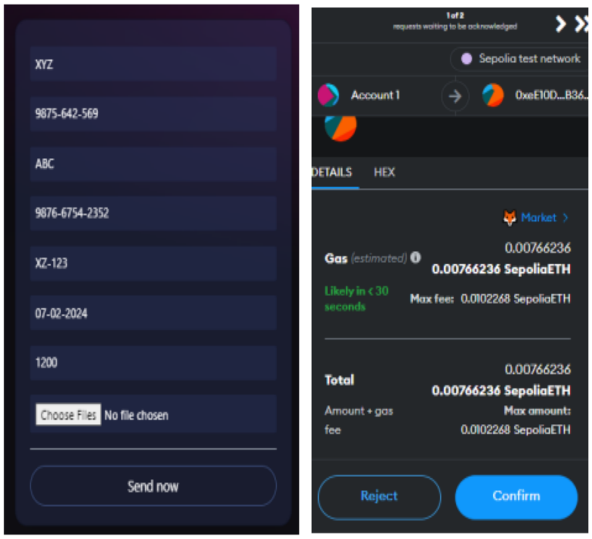
The prevailing methods for recording purchase details often depend on centralized databases, exposing vulnerabilities to security breaches and unauthorized data modifications. The innovative approach advocated in this document proposes the adoption of blockchain technology, diverging from the traditional centralized model to embrace a decentralized and distributed ledger system. Smart contracts, a crucial element of this suggestion, add an extra layer of automation to ensure the enforcement of predefined rules, thereby maintaining the integrity and transparency of purchase records. Additionally, the incorporation of encryption enhances the security of stored data, protecting it from unauthorized access and tampering. A distinctive aspect of this suggested system is the introduction of a ”digital ownership certificate” as a robust authentication mechanism. This certificate provides each transaction with a unique and verifiable digital signature, strengthening the overall security framework. The system's user-friendly search functionality, equipped with various parameters, facilitates the easy and efficient retrieval of specific purchase details to meet diverse user needs. Beyond its immediate application in purchase information management, the blockchain-based platform has broader implications, particularly in sectors like insurance. By offering a decentralized alternative, the system reduces costs associated with intermediaries and improves transaction transparency, fostering trust among parties involved. The integration of smart contracts through the Ethereum blockchain, known for its adaptability, ensures the seamless execution of predefined rules in a secure and transparent manner. The advanced search features, coupled with an intuitive interface, contribute to the overall efficiency of managing, accessing, and securing purchase data, making the proposed system a comprehensive solution to overcome the limitations of current information storage methods.



Ownership Certificate

Purchase ID: 1021
Private Key: J4QMKGYa_jEadybccFM6f

Fig. 5. Digital Ownership Certificate.



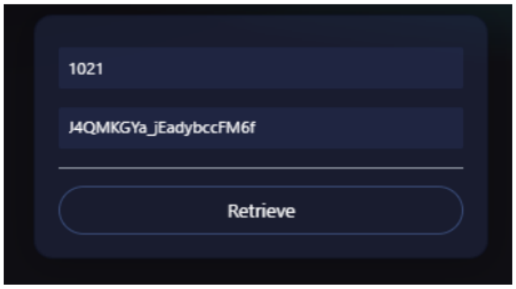
XYZ
9875-642-569
ABC
9876-6754-2352
XZ-123
07-02-2024
1200
Choose Files No file chosen

1 of 2
requests waiting to be acknowledged
Sepolia test network
Account 1 → 0xeE10D...B36...

Gas (estimated) 0.00766236
0.00766236 SepoliaETH
Likely in < 30 seconds
Max fee: 0.0102268 SepoliaETH

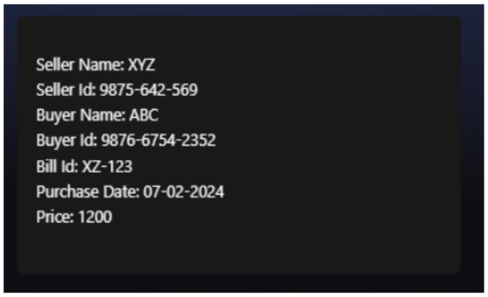
Total 0.00766236
0.00766236 SepoliaETH
Amount + gas fee
Max amount: 0.0102268 SepoliaETH

Fig. 6. Enter Transaction details in Metamask.



1021
J4QMKGYa_jEadybccFM6f

Fig. 7. Retrieve Details through public ID and private key.



Seller Name: XYZ
Seller Id: 9875-642-569
Buyer Name: ABC
Buyer Id: 9876-6754-2352
Bill Id: XZ-123
Purchase Date: 07-02-2024
Price: 1200

Fig. 8. Retrieved transaction details.

5. Conclusion

This research aims to introduce a decentralized framework for the insurance sector, eliminating the need for intermediary entities. The main objective was to create a design and prototype for an insurance platform based on blockchain and driven by the community. The study addresses a gap in existing literature by focusing on community-driven platform designs and implementations in the insurance domain. The goal is to highlight the potential of blockchain technology as a decentralized alternative to the traditional centralized insurance model. The evaluation of the system indicates that adopting a blockchain approach was effective in achieving the outlined research objectives.

6. Future Work

To augment the proposed model further, we can incorporate digital gold transactions. Digital gold serves as an alternative to obtaining physical gold, enabling individuals to conduct online transactions. The corresponding value is securely stored as physical gold in a protected vault. The minimum purchase threshold is as low as one rupee, providing customers with the flexibility to sell the entire quantity or a fraction at prevailing market rates. All gold acquired through this approach is government-certified, ensuring 24K purity and mitigating the risk of fraudulent activities. Noteworthy features encompass the option for investors to receive physical delivery at their doorstep, the ability to invest a minimal amount of just one rupee, and the potential to use digital gold as collateral for online loans. The credibility and purity of the gold are assured, with secure storage in fully insured facilities. Furthermore, digital gold can be exchanged for physical jewelry, gold coins, and bullion.

References

[1] Dorri, A., Steger, M., Kanhere, S., and Jurdak, R. (2022, April). ”Innovative Approaches to Enhance Security and Privacy in the Automotive Industry Using Blockchain.” Forthcoming in IEEE Communications Magazine, 55(04).

[2] Vahdati, M., Gholizadeh HamlAbadi, K., Saghiri, A. M., and Rashidi, H. (2020). ”A Framework for Self-Organized Insurance Utilizing the Internet of Things and Blockchain.” Presented at the 2020 IEEE 6th International Conference on Future Internet of Things and Cloud (Fi-Cloud), pp. 169–175.

[3] Raikwar, M., Mazumdar, S., Ruj, S., Sen Gupta, S., Chattopadhyay, A., and Lam, K.-Y. (2021). ”Integration of Blockchain to Streamline Insurance Processes.” Proceedings of the 2021 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–4.

[4] Demir, M., Turetken, O., and Ferworn, A. (2022). ”Promoting Transparency in Vehicle Insurance Management through Blockchain.” Presented at the 2022 Sixth International Conference on Software Defined Systems (SDS), pp. 213–220.

[5] Oham, C., Jurdak, R., Kanhere, S. S., Dorri, A., and Jha, S. (2019). ”B-fica: A Blockchain-Based Framework for Claim and Adjudication in Auto Insurance.” Proceedings of the 2019 IEEE International Conference on Internet of Things (iThings), Green Computing and Communications (GreenCom), Cyber, Physical and Social Computing (CPSCom), and Smart Data (SmartData), pp. 1171–1180.

[6] Roriz, R., and Pereira, J. L. (2022, January). ”Addressing Insurance Fraud in the Vehicle Sector through a Blockchain-Based Approach.” Published in Procedia Computer Science, 164, 211–218.

[7] Yang, Z., Zheng, K., and Yang, K. (2022, October). ”Establishing a Reputation System for Evaluating Data Credibility in Vehicular Networks Using Blockchain.” pp. 1–5.

[8] Li, L., Liu, J., Cheng, L., Qiu, S., Wang, W., Zhang, X., and Zhang, Z. (2022). ”Creditcoin: A Privacy-Preserving Blockchain-Based Incentive Network for Smart Vehicle Communications.” Published in IEEE Transactions on Intelligent Transportation Systems, 19(7), 2204–2220.