Journal of Computer Science

Research Article

Optimized Vehicle Insurance Claim and Settlement Procedures Using IOT Sensors on a Blockchain-Based Platform

Preeti Sharma[1], Meenakshi Malik[2], Chander Prabha[3], Ibrahim Aljubayri[4], Retinderdeep Singh[3] and Mohammad Zubair Khan[5]

[1]*School of Computing Science and Engineering, Sharda University, Greater Noida, UP, India*
[2]*Department of CSE, BML Munjal University, Gurugram-122001, India*
[3]*Department of Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India*
[4]*Department of Computer Science and Information, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11432, Saudi Arabia*
[5]*Faculty of Computer and Information Systems, Islamic University of Madinah, Madinah 42351, Saudi Arabia*

Article history
Received: 28-06-2025
Revised: 25-08-2025
Accepted: 13-12-2025

Corresponding Authors:
Chander Prabha
Department of Computer Science and Engineering, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India
Email: prabhanice@gmail.com

And,

Mohammad Zubair Khan
Faculty of Computer and Information Systems, Islamic University of Madinah, Madinah 42351, Saudi Arabia
Email: zubair.762001@gmail.com

Abstract: The conventional vehicle insurance claim and settlement landscape is characterised by significant inefficiencies, including cumbersome claim submissions, arbitrary damage assessments, and susceptibility to fraudulent activities. These problems lead to a longer processing time, higher operational cost to the insurers and a reduction in policyholder satisfaction. To address these important challenges, this study proposes a streamlined vehicle insurance claims system that fuses data supplied by IoT sensors and a blockchain-based platform. Our proposed system simplifies the lifecycle of claims by exploiting the immutability and transparency of the distributed ledger of blockchain and automating the smart contracts. IoT sensors can be used to provide objective data on the verification of incidents (real-time data), and smart contracts can be used to pay out claims based on predetermined rules (without human intervention), reducing the risk of fraud. Additionally, a risk management model and mathematical security calculations through hashing and Elliptic Curve Cryptography (ECC) makes resilience stronger. An internet of things (IoT) pilot study of vehicles shows 40% faster claim settlements, higher than 92% fraud detection rates, and increased stakeholder trust. This new strategy is set to improve the safety, effectiveness, and equity of the auto insurance claims, a step towards a more trustworthy and dependable ecosystem to all parties involved.

Keywords: Internet of Things (IoT), Blockchain Technology, Insurance, Underwriting, Risk Management, Fraud Prevention, Claims Processing

Introduction

This research proposes an integrated blockchain-IoT platform for processing vehicle insurance claims, validated through a prototype implementation and empirical testing. The difficulties and complexities associated with filing insurance claims are a well-documented issue. For example, submitting an auto insurance claim typically involves multiple steps: gathering documents from various offices, organizing them chronologically, and submitting them to the appropriate authorities, often followed by a police verification requested by the insurer.

Blockchain technology offers significant advantages in streamlining these procedures and addressing related challenges. It has the potential to facilitate industrial integration, improve information sharing across inquiry departments, and simplify how insurers access verified data. Internet-based insurance models play a key role here. This study incorporates both blockchain and smart contract technologies, which are explained in the following sections. These technologies are particularly valuable because they enable solutions for online underwriting challenges, provide enhanced supervision capabilities, can be applied to address risk management issues, and support effective anti-money laundering efforts.

SCIENCE Publications

© 2026 Preeti Sharma, Meenakshi Malik, Chander Prabha, Ibrahim Aljubayri, Retinderdeep Singh and Mohammad Zubair Khan. This open-access article is distributed under a Creative Commons AAAttribution (CC-BY) 4.0 license.

Background

Blockchain is a transformative technology with the potential to fundamentally alter the nature of business, and its impact is expected to grow significantly in the coming decades. By enabling a decentralized and distributed digital ledger, blockchain enhances transparency, data security, and integrity through its immutable and unforgeable structure. The process by which blocks are validated is illustrated in Fig. 1. Once a block is authorized, it is broadcast to every node in the network. Each node then verifies the transaction, and participants may receive a reward for their validation work before the block is finalized and appended to the existing blockchain.

Blockchain Technology

Blockchain technology functions as a continuously growing database of records, referred to as blocks, which are linked and encrypted to ensure security (Figure 2). Each block typically contains a timestamp, immutable transaction data, and the cryptographic hash code of the preceding block. The concept of blockchain was introduced by Nakamoto in 2008. At its core, blockchain is a distributed ledger of transactions or events, commonly known as Distributed Ledger Technology (DLT). As such, blockchain technology offers a decentralized registry with distributed data control, ensuring information security, transparency, integrity, and resistance to tampering and forgery. It provides high efficiency and low operational costs while remaining programmable, features that enhance both flexibility and reliability. Unlike traditional centralized databases, blockchain enables transparent, secure, decentralized, efficient, and cost-effective transaction tracking.

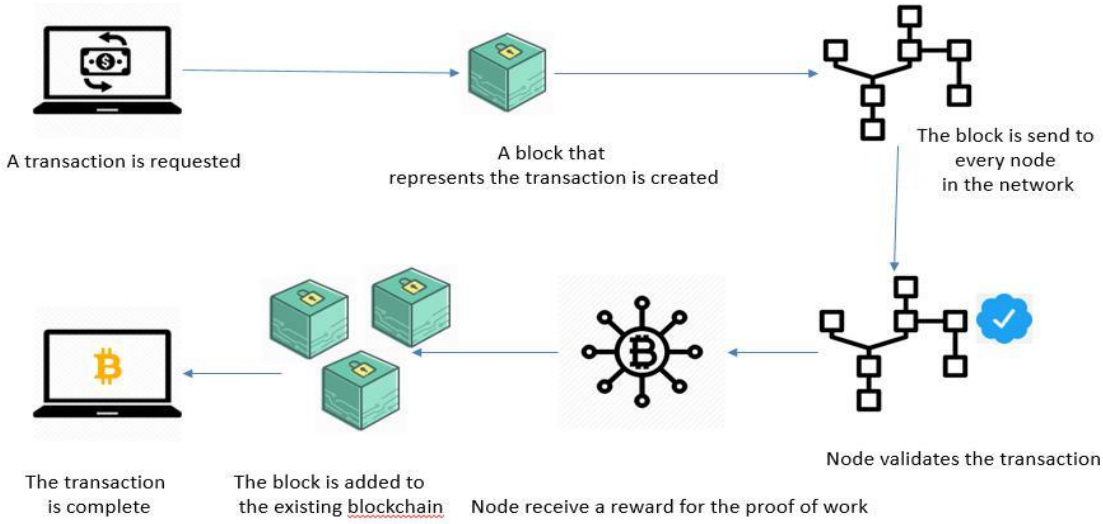

Fig. 1: Blockchain Approval Process

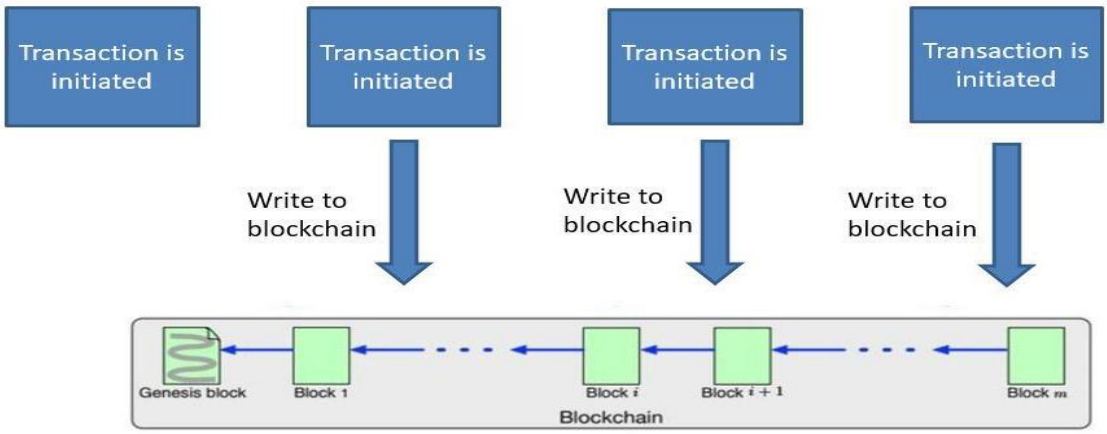

Fig. 2: Connected Blocks

Smart Contract

Smart contracts have significantly advanced blockchain technology by enabling automated, self-executing agreements. First conceptualized in the 1990s, a smart contract is a computerized transaction protocol that executes the terms of an agreement. These contracts encode contractual provisions into logical conditions, for instance, automatically imposing a penalty when a party violates the agreement. The complete lifecycle of a smart contract comprises four stages, as depicted in Figure 3.

When integrated with blockchain technology, smart contracts become fully functional. Legal clauses are translated into executable computer code while preserving the original contractual logic through programmatic structures such as conditional (if-else) statements. Each action performed under the contract is recorded as an irreversible transaction on the blockchain, ensuring both transparency and immutability. Smart contracts also incorporate access control mechanisms and automated enforcement protocols. Developers can assign specific permissions for each contract function, while the embedded enforcement logic guarantees that contractual obligations are fulfilled exactly as intended. Once a predefined condition is satisfied, the corresponding clause is triggered automatically, executing the required operation without the need for intermediaries.

IoT and Blockchain Integration

Recent advancements in Information and Communication Technology (ICT) have accelerated the transition from traditional computer-aided manufacturing to smart manufacturing, characterized by data-driven decision-making. The Internet of Things (IoT) plays a pivotal role in this paradigm shift by forming a Cyber-Physical System (CPS) that bridges the physical industrial world with the computational space of digital systems. IoT holds significant potential to enhance various commercial sectors, including manufacturing, logistics, food industries, and utilities. Its primary objectives are to improve throughput and operational efficiency, reduce machine downtime, and enhance product quality.

IoT systems are distinguished by several key characteristics: decentralization of system architecture, diversity of devices and platforms, heterogeneity of generated data, and network complexity. However, these same features also give rise to significant challenges, including limited interoperability among heterogeneous IoT systems, resource constraints on IoT devices, and vulnerabilities related to privacy and security. Figure 4 illustrates the concept of Blockchain of Things, which integrates blockchain technology with IoT environments to address these challenges.

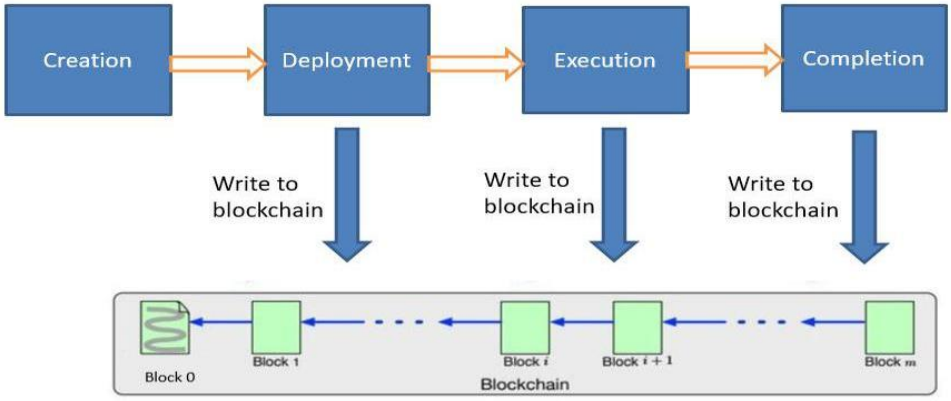

Fig. 3: Smart Contracts Life Cycle

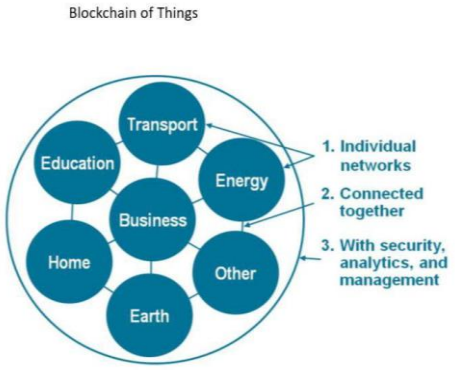

Fig. 4: Blockchain of Things

The emergence of blockchain technology presents a promising opportunity to address the aforementioned challenges associated with IoT. At its core, a blockchain is a distributed ledger that spans the entire network, enabling decentralized consensus. This allows transactions to be initiated and authenticated within a mutually distrusting distributed system without the need for a trusted third party. Unlike traditional transaction management systems that rely on centralized validation, blockchain facilitates decentralized verification, thereby reducing operational costs and eliminating the performance bottlenecks inherent to central authority models.

Problem Statement

According to the International Association of Insurance Supervisors (IAIS), an estimated 20 to 30 percent of insurance claims may be fraudulent. Such fraud is often driven by a small subset of dishonest or uninformed policyholders. A key contributing factor is the lack of transparency and information sharing among insurers. For instance, even if one company blacklists a policyholder, other insurers may continue to engage with that individual without knowledge of their history. This information asymmetry undermines the industry's ability to assess risk accurately and prevent moral hazard.

The current insurance landscape is further challenged by complex and time-consuming underwriting processes, coupled with inadequate monitoring mechanisms across companies. These limitations make it difficult to evaluate applicants' risk profiles effectively and address emerging threats, such as the misuse of online insurance platforms for money laundering.

In the specific context of auto insurance, the interaction among claimants, vehicle service providers, and insurance companies forms a triangular relationship fraught with inefficiencies. At nearly every stage, stakeholders encounter fragmented services and procedural delays. Insurers also bear significant operational costs, particularly in areas such as data analysis, claim inspection, payment processing, database management, and contract administration.

A life insurance example illustrates the broader issue: claimants often face delays while awaiting police verification, a prerequisite imposed by the insurer before disbursement. Similarly, in vehicle insurance, the current claims process is hindered by cumbersome procedures and protracted reimbursement timelines, underscoring the urgent need for more streamlined and transparent solutions.

Objective

This study is designed to achieve several key objectives. First, it seeks to conduct a comparative analysis between conventional insurance policies and those integrated with blockchain technology, highlighting the potential advantages and transformative impact of blockchain adoption. Second, the research aims to leverage smart contracts as a mechanism for enhancing transparency and automation in claimant settlement processes, thereby reducing delays and improving trust among stakeholders.

Additionally, the study focuses on developing a claims management platform that facilitates seamless submission of claims using IoT devices installed in policyholders' vehicles. This platform will enable the processing of vehicle telematics data to support more accurate and efficient claims handling. Ultimately, this research demonstrates how the integration of blockchain and IoT can revitalize the insurance ecosystem, driving innovation and operational advancements across the insurance sector.

Contribution of the Paper

This research highlights several key contributions of blockchain technology to the insurance sector. First, the integration of blockchain-based smart contracts can significantly enhance the efficiency of claims settlement by automating verification and payment processes. Second, the inherent security features of blockchain help alleviate policyholders' concerns regarding data privacy and protection. Third, blockchain technology addresses the longstanding issue of mistrust between policyholders and insurers by enabling transparent, immutable, and verifiable transactions. Fourth, it ensures traceability across the sales chain, thereby preventing data manipulation and fraud.

Beyond these direct applications, blockchain has emerged as a transformative trend across multiple industries, offering a reliable mechanism for maintaining decentralized databases. Its core attributes, decentralization, trustworthiness, immutability, transparency, and traceability, are equally valuable in enhancing the structural efficiency, flexibility, and transparency of services, including those provided by government institutions. By adopting blockchain, governments can improve service delivery while fostering greater public trust and knowledge. Furthermore, the integration of blockchain into public sector operations aligns with the global movement toward Internet+ applications, a strategic initiative supported by governments worldwide to drive digital innovation.

Literature Review

Researchers and industry specialists are increasingly exploring the potential of blockchain and IoT technologies within the insurance sector. A growing body of literature examines how these technologies can be leveraged to address the challenges outlined above, highlighting the transformative advantages they offer in enhancing efficiency, transparency, and trust across insurance operations.

Insurance Systems Powered by Blockchain

Several studies have proposed blockchain-based insurance systems that utilize smart contracts to automate key processes such as underwriting, risk assessment, and claims settlement (Amponsah et al., 2021; 2022). By enabling automatic transaction execution and enforcing policy conditions, smart contracts help reduce operational costs and improve overall efficiency.

In a related study, researchers explored blockchain-based solutions aimed at protecting the National Health Insurance Scheme (NHIS) from financial risks and cyber

threats. The DeLone and McLean Information Systems Success Model was employed to evaluate system effectiveness, with findings indicating that user satisfaction and information quality significantly influenced the system's success (Amponsah et al., 2022).

Despite these advancements, the insurance sector has received comparatively limited attention in blockchain research. This study seeks to address that gap by demonstrating how investments in blockchain technology can yield substantial benefits for the insurance industry. Prior work has already illustrated the potential of blockchain to enhance various subprocesses within insurance operations (Amponsah et al., 2021).

Insurance Powered by IoT and Blockchain

The integration of IoT devices with insurance systems has been increasingly explored to enable real-time data collection and analysis, facilitating more accurate risk assessment and proactive risk mitigation. By capturing valuable information on driver behavior, vehicle performance, and environmental conditions, IoT devices allow insurers to tailor products more precisely and potentially prevent accidents or incidents before they occur.

However, despite their ability to sense and record data, IoT devices often face processing and security limitations due to their constrained computational capacity. Traditional cryptographic methods may prove inadequate for transmitting and storing sensitive information such as medical records. In this context, blockchain technology offers a decentralized storage solution that ensures data authenticity, immutability, and confidentiality. For instance, a blockchain-based IoT-EHR architecture has been developed to enhance the security and reliability of electronic health record systems, ensuring both patient privacy and effective data management (Alam et al., 2023).

To further safeguard highly sensitive health information, recent research has combined Proof of Work (PoW) with Practical Byzantine Fault Tolerance (PBFT) within smart contracts. While PoW and PBFT achieved accuracy rates of 92.75% and 90.15%, respectively, the proposed hybrid PBFT-PoW model attained an accuracy of 99.88%. This integration of a hybrid consensus protocol with blockchain technology effectively addressed critical concerns related to safety, security, and privacy in electronic applications (Palanikkumar et al., 2023).

In a related application, an electronic device equipped with sensors collects data on both passengers and vehicle conditions, enabling automatic adjustments to insurance coverage based on real-time circumstances and preferences. This approach aims to reduce policy modification costs and minimize the risk of insurance fraud (Lamberti et al., 2018).

Regulatory Aspects to Take into Account

The regulatory landscape surrounding the adoption of IoT and blockchain technologies in the insurance industry is rapidly evolving (Kapadiya et al., 2022). As these emerging technologies gain broader acceptance, regulators are actively investigating frameworks to ensure consumer protection, data privacy, fraud detection, and compliance with existing insurance requirements (Setyowati et al., 2020). Blockchain technology facilitates the creation of trustworthy, decentralized networks, while IoT environments often involve diverse and potentially unreliable devices. In response, recent research has focused on leveraging existing frameworks to establish a decentralized global IoT marketplace, where consumers pay for data and device owners are compensated for providing it. Such systems typically employ a distributed oracle layer, powered by a global network of IoT devices, operating on top of smart contracts to ensure reliability and transparency (Gigli et al., 2023; Khatun et al., 2023).

Beyond regulatory considerations, blockchain holds significant promise across multiple sectors by advancing the understanding and application of parametric insurance models, particularly within the transportation industry (Dutta et al., 2023; Lamberti et al., 2018). This approach enables automated, condition-based payouts triggered by verifiable data, reducing administrative overhead and improving response times. The potential applications of parametric insurance extend well beyond transportation, encompassing diverse fields such as manufacturing, tourism, catastrophe risk management, agriculture, and aviation (Dutta et al., 2023; Karmakar et al., 2023).

The insurance sector continues to rely on insufficient and outdated fraud prevention mechanisms, contributing to persistent challenges in data security and fraudulent activities. In this context, blockchain technology has emerged as a transformative innovation, often compared to the internet and the combustion engine in terms of its potential to disrupt established industries (Kar and Navin, 2021; Mateen et al., 2023; Pagano et al., 2019).

A review of the existing literature reveals a notable gap in automated solutions for emergency response and claims processing, particularly in the domain of intelligent fire detection and insurance frameworks. Few studies have addressed the integration of automated alerts to fire departments alongside prompt claims resolution (Bhawana et al., 2023). In response, recent research has proposed the use of smart contracts to automate both insurance claim procedures and notifications to fire service authorities (Shetty et al., 2022; Alnuaimi et al., 2022). The performance of such proposed solutions is typically evaluated through security analysis and comparison with existing systems (Trivedi and Malik, 2022).

By addressing the inherent limitations of centralized systems, blockchain technology holds the potential to

fundamentally transform the insurance industry. Traditional insurance processes are often characterized by centralization, high costs, and tedious paperwork, resulting in significant frictional costs and inefficiencies for customers. Blockchain-based platforms offer a means to enhance the efficiency, transparency, and trustworthiness of insurance transactions (Alwis and Jinasena, 2022). However, due to the complexity and trust requirements of certain insurance products, traditional firms may be hesitant to adopt such innovative contracts.

The acceptability of blockchain technology in specific contexts has also been explored. A quantitative study conducted on 213 enterprises across various industries in Lebanon examined the factors influencing the adoption of blockchain for business interruption insurance amid sanitary and economic crises. The findings revealed that acceptability varied according to sociodemographic factors. In this challenging environment, decentralized finance (DeFi) and smart contracts have been proposed as viable solutions to address high insurance premiums and currency depreciation (Boustani and Elisabetta, 2022).

Traditional Insurance Policy vs Proposed Insurance Technology

The traditional manual approach to insurance policy settlement is widely recognized as lengthy and inefficient (Hassan et al., 2021). The complexity of the settlement process is further compounded by hidden terms imposed by insurers and allegations of fraud raised by policyholders. In response to these challenges, blockchain technology and smart contracts offer transformative potential by providing irreversible data storage, enhanced privacy, authenticity, integrity, and overall transactional efficiency (Ananna et al., 2023).

Another critical yet often overlooked area is the subrogation process in insurance, which remains tedious and protracted, leading to substantial administrative costs and delays in claims processing. Despite the emergence of various blockchain-based proposals for general insurance, the specific issue of subrogation has not been adequately addressed in existing research (Bhadra et al., 2022). This gap highlights the need for further exploration of blockchain applications to streamline subrogation and improve end-to-end claims management.

Hash Key Generation and Smart Contract

In a recent study focused on medical record platforms, researchers developed a smart contract algorithm designed to manage access to healthcare systems by addressing identity and reliability concerns while ensuring immutable execution. The algorithm was implemented using the Solidity programming language within a permissioned, private architecture. Additionally, a novel consensus mechanism incorporating a hash function was introduced, demonstrating a 22% improvement in processing speed and significantly reduced computational resource consumption compared to existing approaches (Mendoza Arvizo et al., 2023).

Collectively, the existing body of research underscores the transformative benefits of blockchain technology, including enhanced transparency, decentralization, and trust (Amponsah et al., 2021; Mateen et al., 2023). Simultaneously, IoT has enabled real-time monitoring capabilities across various industries (Lamberti et al., 2018). In the healthcare domain, the integration of blockchain and IoT has shown promise in improving data privacy and preventing fraud (Alam et al., 2023; Palanikkumar et al., 2023). Despite these advancements, insurance-specific applications of integrated blockchain-IoT systems remain comparatively underexplored.

This study addresses that gap by extending prior conceptual frameworks through the implementation and empirical validation of a blockchain-IoT hybrid platform tailored for vehicle insurance. The research advances the state of the art in several key ways: first, by demonstrating a functional prototype that integrates both blockchain and IoT technologies; second, by presenting a comprehensive risk management framework tailored to insurance contexts; third, by applying mathematical cryptographic computations to enhance system security; and finally, by providing pilot study results that demonstrate measurable improvements in operational efficiency and reductions in fraudulent activities.

Materials and Methods

The research design outlines the overall structure and approach adopted in this study. A mixed-methods strategy is employed, combining quantitative simulations with qualitative feedback research procedures. This dual approach enables a comprehensive investigation: quantitative methods provide statistical analysis for objective measurements, while qualitative approaches facilitate an in-depth understanding of subjective factors relevant to the research context.

Mathematical Computation for Security

- Hashing Function: $H(x) = SHA256(data)$, ensuring tamper-proof records
- ECC: $y^2 = x^3 + ax + b$, ensuring secure key exchange with lower computational overhead
- Computational Complexity
  - SHA-256 hashing → $O(n)$
  - ECC encryption/decryption → Based on discrete log problem, infeasible to break with current computing
- To ensure tamper-proof claim records, the system applies a cryptographic hash function
- $H(x) \rightarrow \{0,1\}^n$
- where $x$is the transaction data and n is the hash length. Each block B_i stores the tuple

- $B_i = (Tx_i, H(B_{i-1}), Timestamp, Nonce)$
- Security is guaranteed since altering any transaction Tx_i requires recomputing all subsequent hashes. The Proof-of-Work consensus ensures that the expected probability *P*of a malicious node successfully rewriting history decreases exponentially
- $P \approx \left(\frac{q}{p}\right)^z$
- where q is the attacker's hashing power, p the honest network power, and z the number of blocks to be altered. With $q < 0.5, P \to 0$ as z increases, confirming blockchain immutability

Testing Environment and Pilot Study

- Blockchain Platform: Hyperledger Fabric with private Ethereum testnet
- IoT Devices: Raspberry Pi with GPS and accelerometer
- Software Tools: Solidity for smart contracts, Python for sensor integration
- Pilot Setup: 10 vehicles instrumented with IoT devices. Controlled crash scenarios were simulated, and claims auto-verified

By utilizing the special qualities of blockchain technology and IoT, the suggested blockchain-based insurance solution seeks to overcome the aforementioned issues. There are three main parts of the system.

Safe Network for Blockchain

The foundation of the system is a tamper-proof and secure blockchain network that offers a distributed and transparent ledger for all insurance transactions (Lamberti et al., 2018; Kapadiya et al., 2022). By guaranteeing the data's traceability and immutability, this promotes participant accountability and confidence (Setyowati et al., 2020).

Autonomous Smart Contracts

Underwriting, risk assessment, and claims settlement are just a few of the insurance operations that can be automated with smart contracts self-executing contracts kept on the blockchain (Gigli et al., 2023). Smart contracts lower operating expenses and increase efficiency by carrying out transactions automatically and enforcing the conditions of insurance policies (Khatun et al., 2023; Dutta et al., 2023).

IoT Devices Installed in Assets Under Insurance

In order to gather real-time data on a variety of factors, Internet of Things (IoT) sensors are put in insured assets, including machinery, residences, and cars (Lamberti et al., 2018; Dutta et al., 2023). The blockchain network receives this data, which gives insurers insightful information for risk assessment, proactive risk reduction, and customized insurance products (Karmakar et al., 2023).

Architecture and Design of Systems

To ensure that the communication between the blockchain network, smart contracts, and the Internet of Things devices is safe and effective, the system architecture was carefully constructed. Data security and privacy are accorded a high priority during the design process.

The architecture of the proposed blockchain-based insurance system can be seen in Fig. 5 and in this diagram, the interactions between smart contracts, the IoT devices, insurance players, and blockchain network are visible.

Development of Smart Contracts

A computer language like Solidity or Vyper is used to create smart contracts, which are used to automate several insurance procedures. To guarantee their functioning and security, these contracts undergo extensive testing.

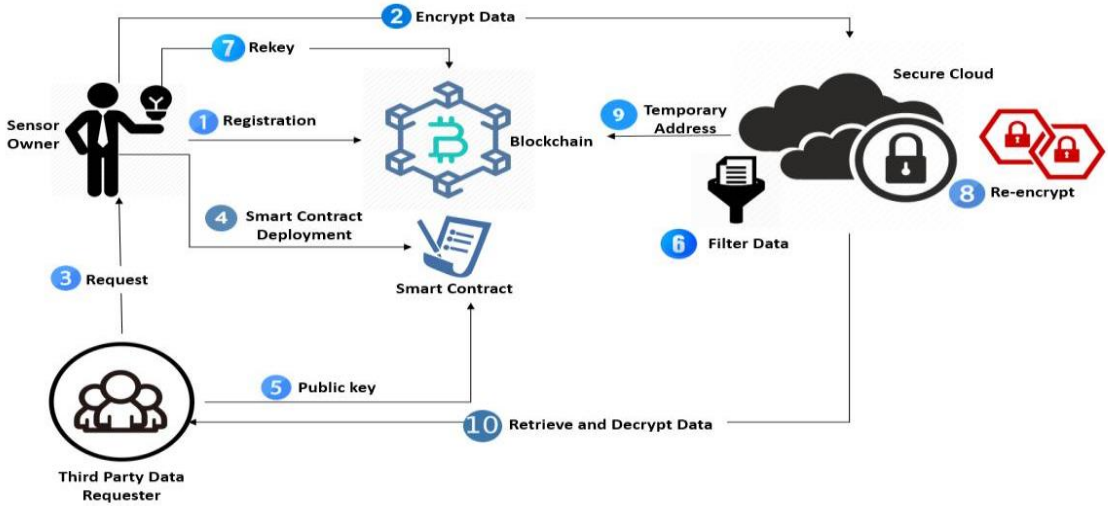

Fig. 5: The Architecture of a Proposed Blockchain-Based Insurance System

IoT Device Integration

In order to gather data from insured assets in real time, IoT devices are incorporated into the system. To guarantee safe and dependable data transfer to the blockchain network, data transmission protocols are developed. The insured asset and the required data points will determine the precise kind and setup of IoT devices. IoT sensors, for example, can gather information on driving habits, the position of the vehicle, and the surrounding environment in the context of auto insurance as shown in Fig. 6.

Registration Process

To use the proposed blockchain-based system, the users simply need to open the specific URL of the blockchain network and start the registration process. After visiting the platform, they give crucial vehicle information and account information. Security and integrity are achieved by the system by implementing a proof of work, which is a consensus mechanism implemented by miners in the network. Mutual authentication (MTLS) is used to provide a secure channel of communication between parties. Then, it will generate a personal key, which will give a unique access to the platform. The system will then go ahead to construct a smart contract, which personalizes the best insurance policy depending on the specified information. An extra wave of security is also brought by placing an IoT device in the registered vehicle. This integration elevates the level of data immutability and traceability in that all the information can be accessed safely and can only be accessed by the related private keys. Under this ultimate configuration, users will have a smooth flow through the platform since they can log in with their personal keys. Such a simplified process ensures easy renewal, quick processing of claims and a hassle-free update which is a big leap in the user experience in the vehicle insurance sphere as demonstrated in Fig. 7. The architecture of the system based on blockchain, smart contracts, and IoT creates a solid and safe framework of the insurance policy management.

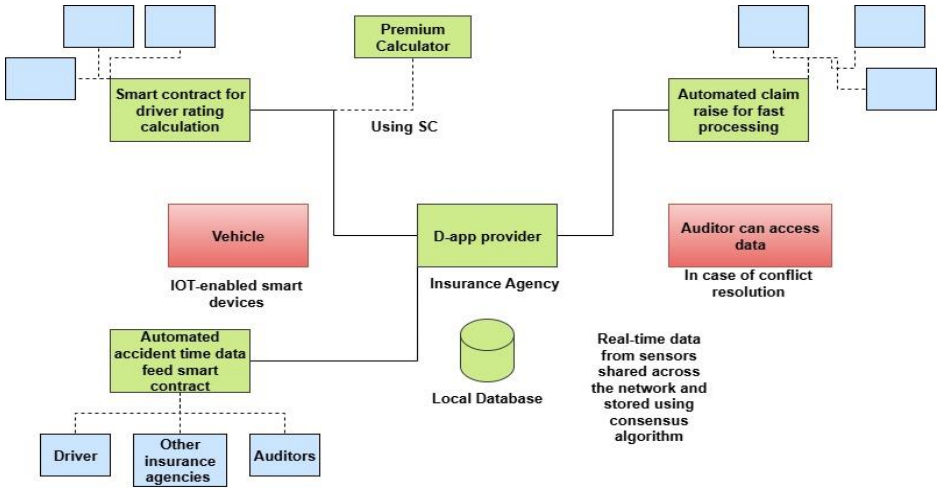

Fig. 6: IoT Device Integration

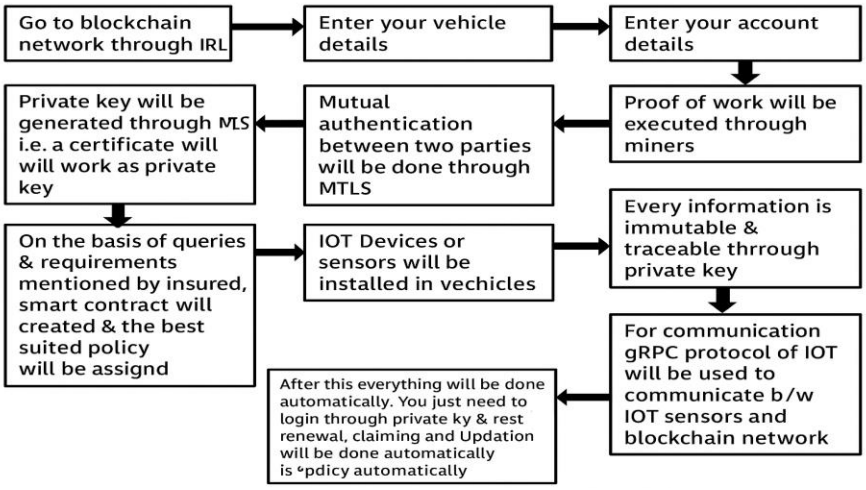

Fig. 7: Registration Process

Claiming Process

When a successful registration process is completed, the insurance claims in the system can be easily initiated through the logging into the blockchain network with the help of the granted certificate. In case of an accident, the corresponding IoT sensors implemented in the car are triggered, which is immediately sent through the blockchain network using a secure communication protocol. The IoT is central to making the process of claims faster since damages are computed with accuracy relying on the real-time data that is given by these sensors. The system, based on this data, creates an autonomous smart contract in the form of a code. This new smart contract is an evolving and self-executing contract, which removes the burdensome questions and voluminous paperwork that are characterized when filing an insurance claim. The resulting smart contract will serve as the only source of truth that will store all the relevant information and whether the claims are to be settled or not. After the smart contract is implemented, the pre-set monetary compensation will be automatically deposited directly into the account of an insured party. It is not just a quick and automated system that will accelerate the claims settlement but will also be much better when it comes to transparency and the burden of administration on the insurance company and the policy holder. Blockchain combined with IoT sensors and smart contracts will change the climate of the insurance business and make it more efficient, secure, and user-friendly as shown in Fig. 8.

System Evaluation and Implementation

Extensive testing is done to test the scalability, security and functionality of the system. The testing scenarios include simulation of various insurance operations, performance of the integration of IoT devices, and testing the communication with smart contracts. Testing is completed after which the system is placed in a safe, supervised environment.

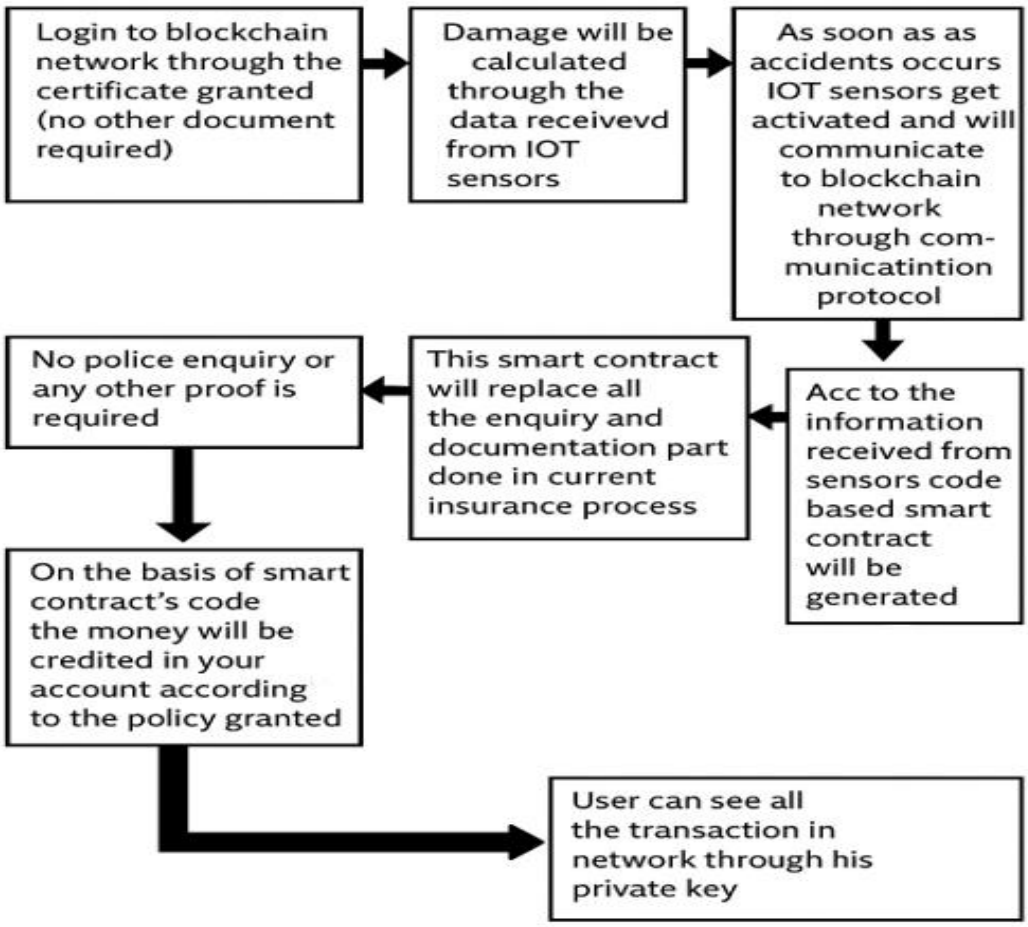

Fig. 8: Workflow for Processing Claims

Results

This section presents the experimental findings obtained from evaluating the proposed system under various parameter configurations. Graphical representations are included to visually illustrate the results and enhance interpretability.

User Interface of Our Proposed System

Figure 9 demonstrates the core blockchain operations relevant to the insurance industry, highlighting key functionalities of the system. The interface enables users to enumerate blockchain nodes, providing an overview of network participants and their roles. Additionally, it allows retrieval of unique node identifiers, ensuring secure and authenticated communication within the network. A ping operation to the blockchain master node is incorporated to verify network connectivity and operational status. Finally, the interface supports access to the most recent block on the blockchain, emphasizing real-time availability of transaction data. Collectively, these operations contribute to the transparency, efficiency, and seamless functioning of the proposed system within the insurance sector.

Fig. 9: Essential Operations for Seamless Insurance Transactions

Fig. 10: Operations performed in Vehicle's Insurance Policy

Figure 10 illustrates the key operations within the vehicle insurance policy framework, beginning with the creation of identity key pairs to enable secure and personalized user access. Through the system, users can initiate the purchase of insurance contracts, a process seamlessly facilitated by blockchain technology. The platform also allows users to view existing insurance contracts, promoting transparency and ease of access. In the event of a claim, the system executes streamlined blockchain operations to support swift and automated claims processing. Together, these functionalities empower users by providing a user-friendly interface for managing insurance policies with enhanced security and operational efficiency.

Figure 11 highlights the creation of key pairs upon network entry, displaying both the private and public keys that constitute the user's identity. This cryptographic pairing strengthens security among network participants by enabling authenticated and encrypted interactions. The private key, known only to the user, ensures personalized access and authorization, while the public key serves as a verifiable counterpart for communication and verification purposes. The seamless generation of these key pairs reinforces the robustness of user authentication, forming the foundation for secure transactions and interactions within the network.

Figure 12 focuses on the process of selecting and submitting an insurance contract within the network. The interface presents four key input fields—owner name, vehicle number, contract name, and contract code—where users enter essential information to initiate a contract. This intuitive design facilitates accurate and complete data submission, streamlining the onboarding process. The inclusion of these fields ensures that ownership details, vehicle specifics, and contract identifiers are clearly captured. By offering a seamless and transparent interface, the system enhances the user experience and supports efficient contract initiation within the blockchain-based insurance network.

Fig. 11: Establishment of Key Pair

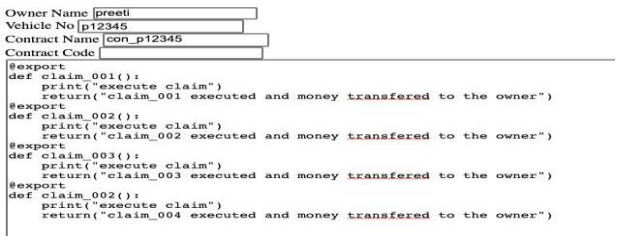

Fig. 12: Selection and Submission of Insurance Contract in Network after entering all the required details

Figure 13 illustrates the process of hash key generation, a fundamental operation within the blockchain system. Hash keys are cryptographic

representations of data, algorithmically generated to uniquely identify information stored on the blockchain. This mechanism is essential for ensuring data integrity and system security, as any alteration to the input data results in a completely different hash output. The figure demonstrates the complexity of the algorithmic process involved in creating these hash keys, providing a visual representation of the underlying mechanism that guarantees the immutability and traceability of information recorded on the blockchain. Hash key generation serves as a cornerstone of blockchain technology, not only ensuring the authenticity of transactions but also reinforcing the decentralized and secure architecture upon which the system is built.

{ "hash": "802abd7583ee95bf1a85e94319a7df6a6870356e535ace9a8827ea67b2cf1996", "result": "None", "stamps_used": 1, "state": [{ "key": "con_p12345.__code__", "value": "@__export('con_p12345')\ndef claim_001():\n return 'claim_001 executed and money transfered to the owner'\n\n\n@__export('con_p12345')\ndef claim_002():\n return 'claim_002 executed and money transfered to the owner'\n\n\n@__export('con_p12345')\ndef claim_003():\n return 'claim_003 executed and money transfered to the owner'\n\n\n@__export('con_p12345')\ndef claim_002():\n return 'claim_004 executed and money transfered to the owner'\n" }, { "key": "con_p12345.__compiled__", "value": { "__bytes__": "e3000000000000000000000000000000000000300000040000007344000000650064008301640164028400830 15a0165006400830164036404840083(} }, { "key": "con_p12345.__owner__", "value": "cda0668a0aef71f7d5ff40d3299e5440c303a85aa74f8091710d25272acc2d15" }, { "key": "con_p12345.__submitted__", "value": { "__time__": [2022, 1, 10, 8, 30, 50, 0] } }, { "key": "con_p12345.__developer__", "value": null }], "status": 0, "transaction": { "metadata": { "signature": "ec9aeec0b6af32185f809815bcd051380c9fbb1e5490f3b0638150c76352d7d3ac06a0485e3abca231f2069ad1f0f46cb4fd2913fc7eb43af48545136522("timestamp": 1641803449 }, "payload": { "contract": "submission", "function": "submit_contract", "kwargs": { "code": "@export\r\ndef claim_001():\r\n return(\"claim_001 executed and money transfered to the owner\")\r\n@export\r\ndef claim_002():\r\n return(\"claim_002 executed and money transfered to the owner\")\r\n@export\r\ndef claim_003():\r\n return(\"claim_003 executed and money transfered to the owner\")\r\n@export\r\ndef claim_002():\r\n return(\"claim_004 executed and money transfered to the owner\")\r\n\r\n", "name": "con_p12345", "owner": "cda0668a0aef71f7d5ff40d3299e5440c303a85aa74f8091710d25272acc2d15" }, "nonce": 1, "processor": "0d04cb6568f18b3086fa8965e3f4b960719a8487fd6ab6c9f9fc59d96dcdc3c8", "sender": "cda0668a0aef71f7d5ff40d3299e5440c303a85aa74f8091710d25272acc2d15", "stamps_supplied": 50000 } }, "timestamp": "Mon, 10 Jan 2022 08:30:51 GMT" }

Fig. 13: Hash key of the generated Block in Blockchain is generated

"{\"masternodes\":[\"0d04cb6568f18b3086fa8965e3f4b960719a8487fd6ab6c9f9fc59d96dcdc3c8\"],\"delegates\":[\"8de249918655b5649906ca060eb1ac7af78d9f363e7bd9ca502f934c09977df9\"]}"

Fig. 14: Methods in Smart contract has been deployed

Figure 14 illustrates the master node selection process, a critical landmark in the blockchain system. This operation is fundamental to maintaining efficiency within the decentralized network, as the master node is responsible for monitoring and authenticating transactions while facilitating consensus among participants. The figure graphically represents the strategy underlying the selection of a master node, a decision that significantly influences network performance and integrity. This process is essential for establishing a robust and reliable blockchain infrastructure, contributing to system stability and the overall effectiveness of decentralized operations within the digital environment.

Figure 15 provides a visual overview of the post-establishment phase of an insurance contract, emphasizing network access following the generation of a key pair. Users are authenticated securely using their unique private keys, ensuring that only authorized individuals gain access. Upon successful authentication, the system allows users to view their public keys, which serve as cryptographic counterparts managed through the private key. This mechanism enhances both security and secure communication within the network. The graphical representation highlights the combination of user-friendly design and robust cryptographic protocols, illustrating a seamless and secure interaction model for managing insurance contracts on the blockchain network.

Fig. 15: Login to the network

Figure 16 demonstrates the derivation of a public key using the corresponding private key, illustrating the cryptographic relationship that underpins secure identity management within the blockchain network. Figure 17 presents the initial state of the blockchain network upon launch, characterized by the absence of additional blocks and a blank transaction hash. This snapshot captures the blockchain prior to any recorded transactions or data entries, highlighting its foundational state. The empty transaction hash signifies that no transactions have yet been recorded, underscoring the transparency and traceability inherent to blockchain systems. Together, these visual examples provide a clear depiction of the blockchain's genesis state, a blank slate awaiting the

sequential addition of immutable, cryptographically linked blocks that will ultimately form a secure and decentralized ledger.

Fig. 16: Information of Key Pair

Fig. 17: Blockchain network setup for Transaction

The master node has been allocated to establish the Proof of Work consensus mechanism. Once the node is synchronized with the network, it undergoes a verification process to confirm its synchronization status before connecting to the user interface via the Sanic API. Upon successful establishment of the node, the network is fully operational and ready to process transactions.

Following network verification, both the master node and delegate nodes are confirmed, and a new block is appended to the blockchain for each of these nodes, with its corresponding hash key generated. Concurrently, additional smart contract functions are triggered for processing. Figure 18 illustrates the automation of smart contracts, highlighting a critical feature of the blockchain system. Smart contracts, self-executing algorithms encoded with predefined conditions, operate automatically once their triggering conditions are met. This automation eliminates manual intervention in insurance-related operations such as claims processing and policy execution. The graphical representation emphasizes the efficiency gains achieved through automation, demonstrating how smart contracts simplify and expedite complex transactions. This not only saves time but also enhances accuracy, establishing a seamless and secure framework for fulfilling contractual obligations within the blockchain network.

Upon transaction completion, the new block is inserted into the blockchain, and the transaction hash is populated with the hash key generated from the preceding transaction.

Figure 19 clearly depicts the transaction process, illustrating the inclusion of a new block within the blockchain. The transaction hash, previously empty, is now populated with the hash key generated from the preceding transaction. This visual representation summarizes the seamless and secure workflow inherent to blockchain operations. The completed transaction hash serves as a cryptographic link connecting the current transaction to the previous one, thereby ensuring the integrity and traceability of the entire transaction history. This illustration reinforces the foundational principles of blockchain technology, emphasizing both the immutable nature of transactions and the interconnected structure of the decentralized ledger.

Figure 20 captures a critical user interaction within the system: an insurance holder accessing the platform to file a claim regarding specific damage. The user interface provides a smooth and secure access procedure, safeguarding the privacy and authenticity of the policyholder. Authentication is performed using the user's private key, which grants access to insurance-related functionalities. This graphical depiction highlights the user-friendly design of the claims management process within the blockchain system, offering a clear and intuitive interface that enables policyholders to navigate the platform and initiate claims efficiently and without unnecessary complexity.

"{\"hash\": \"e0401f75dcac18cd0c5361a296c181b2734eae2c25e43fd617e9d173dd436416\", \"number\": 2, \"previous\":
\"9c963e8120150c52e5de8418b2a85a5dbd7368f377d258413aad8be7bdc8b069\", \"subblocks\": [{\"input_hash\": \"994865603f14171f5124cb43d600263ccf2f874799e687962b996325f2eea07e\",
\"merkle_leaves\": [\"02c71ff9a8bdf3e9d632dc2929d6168d66d08217c96809623237d4984b8ae4db\"], \"signatures\": [{\"signature\":
\"2cf9054b8815b3b919e9eef26be10fb38699a8a15ff3f118f936a6e7cc35c289e9dbb0e49c608ec562d81fff88f30eaea37895b3059ff4e7f83c0233275cdb0d\", \"signer\":
\"8de249918655b5649906ca060eb1ac7af78d9f363e7bd9ca502f934c09977df9\"}], \"subblock\": 0, \"transactions\": [{\"hash\":
\"802abd7583ee95bf1a85e94319a7df6a6870356e535ace9a8827ea67b2cf1996\", \"result\": \"None\", \"stamps_used\": 1, \"state\": [{\"key\": \"con_p12345.__code__\", \"value\":
\"@__export('con_p12345')\\ndef claim_001():\\n return 'claim_001 executed and money transfered to the owner'\\n\\n\\n@__export('con_p12345')\\ndef claim_002():\\n return 'claim_002 executed
and money transfered to the owner'\\n\\n\\n@__export('con_p12345')\\ndef claim_003():\\n return 'claim_003 executed and money transfered to the owner'\\n\\n\\n@__export('con_p12345')\\ndef
claim_002():\\n return 'claim_004 executed and money transfered to the owner'\\n\"}, {\"key\": \"con_p12345.__compiled__\", \"value\": {\"__bytes__\":
\"e300000000000000000000000000000000000300000040000000734400000065006400830164016402840083015a0165006400830164036404840083015a0265006400830164056406840083015a0365(
{\"key\": \"con_p12345.__owner__\", \"value\": \"cda0668a0aef71f7d5ff40d3299e5440c303a85aa74f8091710d25272acc2d15\"}, {\"key\": \"con_p12345.__submitted__\", \"value\": {\"__time__\":
[2022, 1, 10, 8, 30, 50, 0]}}, {\"key\": \"con_p12345.__developer__\", \"value\": null}], \"status\": 0, \"transaction\": {\"metadata\": {\"signature\":
\"ec9aecc0b6af32185f809815bcd051380c9fbb1e5490f3b0638150c76352d7d3ac06a0485e3abca231f2069ad1f0f46cb4fd2913fc7eb43af48545136522d10a\", \"timestamp\": 1641803449},
\"payload\": {\"contract\": \"submission\", \"function\": \"submit_contract\", \"kwargs\": {\"code\": \"@export\\r\\ndef claim_001():\\r\\n return(\\\"claim_001 executed and money transfered to the
owner\\\")\\r\\n@export\\r\\ndef claim_002():\\r\\n return(\\\"claim_002 executed and money transfered to the owner\\\")\\r\\n@export\\r\\ndef claim_003():\\r\\n return(\\\"claim_003 executed and
money transfered to the owner\\\")\\r\\n@export\\r\\ndef claim_002():\\r\\n return(\\\"claim_004 executed and money transfered to the owner\\\")\\r\\n\\r\\n\", \"name\": \"con_p12345\", \"owner\":
\"cda0668a0aef71f7d5ff40d3299e5440c303a85aa74f8091710d25272acc2d15\"}, \"nonce\": 1, \"processor\": \"0d04cb6568f18b3086fa8965e3f4b960719a8487fd6ab6c9f9fc59d96dcdc3c8\",
\"sender\": \"cda0668a0aef71f7d5ff40d3299e5440c303a85aa74f8091710d25272acc2d15\", \"stamps_supplied\": 50000}}}]}]}"

Fig. 18: Master node selection

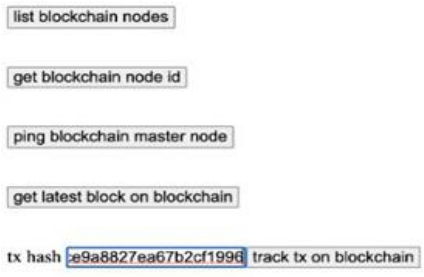

Fig. 19: Master node selection

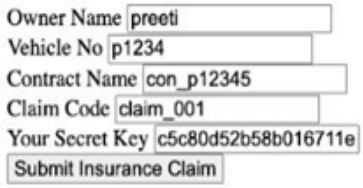

Fig. 20: User Interface for Insurance Holder

Figure 21 illustrates the generation of a hash key in response to a submitted claim request. Once generated, the hash is transmitted from the front end of the insurance contract interface to the back end, where it is recorded on the blockchain alongside the latest request. The current transaction and smart contract details, corresponding to the selected claim, are now visible on the blockchain network using this hash key as a reference.

Following claim selection, a series of methods and functions are initiated on the network to facilitate further processing. As shown in Figure 22, if no contract name is entered by the user, the system prevents block addition and displays an error message indicating incorrect or missing information, thereby ensuring data integrity and guiding the user toward successful submission.

When all details are correctly provided and the claim request aligns with the verified information on the network, mutual authentication is completed, and the transaction is processed successfully. Figure 23 captures this pivotal moment, depicting the successful execution of a transaction and the subsequent addition of a new block to the blockchain. The details of the successful transaction are visible on the network, and the claim is automatically processed, with the required amount credited to the policyholder's bank account. This visual representation underscores the seamless, secure, and efficient nature of blockchain-based transactions. Each successful transaction contributes to the ever-expanding and immutable chain, reinforcing the principles of transparency, security, and decentralized trust that define blockchain technology.

"{\"hash\": \"2c57b492536cb3975d275a0f5e89766cc25cba25c3f3b84154825e11753e0693\", \"result\": \"claim_001 executed and money transfered to the owner\", \"stamps_used\": 1, \"state\": [], \"status\": 0, \"transaction\": {\"metadata\": {\"signature\": \"9e57f3b022e35f78890a35684bef51327d2300be5b87ac02cc9c285c8fd1a48aa972198eb26a5988031eacb5d532002bf7d37847c5cc75bb4500965c28948504\", \"timestamp\": 1641805070}, \"payload\": {\"contract\": \"con_p12345\", \"function\": \"claim_001\", \"kwargs\": {}, \"nonce\": 2, \"processor\": \"0d04cb6568f18b3086fa8965e3f4b960719a8487fd6ab6c9f9fc59d96dcdc3c8\", \"sender\": \"cda0668a0aef71f7d5ff40d3299e5440c303a85aa74f8091710d25272acc2d15\", \"stamps_supplied\": 50000}}}"

Fig. 21: Information about the new transaction on Blockchain

{ "hash": "4497d0bc8509a5f2a2e9c427844e69bea86d64a1241547a491aeea9bdfb5e83e", "result": "ModuleNotFoundError(\"No module named 'con_p1234'\")", "stamps_used": 1, "state": [{ "key": "currency.balances:94cf8d5a111a77a717575fc119d68719584c5188ea256511a0263358e34cf33c", "value": null }], "status": 1, "transaction": { "metadata": { "signature": "81464d3a77a37b65a780668ee6a24a043f1304bd20ed4cdbd85c6e583245bf05bd78b13a710a404a6949e4018850e44553c3467c0f2cfba7373976277fc44d06", "timestamp": 1641805699 }, "payload": { "contract": "con_p1234", "function": "claim_001", "kwargs": {}, "nonce": 1, "processor": "0d04cb6568f18b3086fa8965e3f4b960719a8487fd6ab6c9f9fc59d96dcdc3c8", "sender": "94cf8d5a111a77a717575fc119d68719584c5188ea256511a0263358e34cf33c", "stamps_supplied": 50000 } }, "errors": ["This transaction returned a non-zero status code"], "timestamp": "Mon, 10 Jan 2022 09:08:21 GMT" }

Fig. 22: Information about the new transaction on Blockchain

"{\"hash\": \"b1230b34e163644c861ed12cd33f5283c914602db2d134ee836c05dd8d602cdb\", \"number\": 7, \"previous\": \"c06e4e1709739640baca99971d3d1840a95de476f3c1824438d81e96ec6e56cc\", \"subblocks\": [{\"input_hash\": \"2431afac46fbc265c93997786be9b4d1d221bca89868cff1ff84226a6269f90f\", \"merkle_leaves\": [\"479c6b740aef3a46c553c05c49d376ba468fa490e5d70565f5e501a05630e676\"], \"signatures\": [{\"signature\": \"4561dd9cb3756a5c974b9e4e7b2afa1206462b261f0f4a99eeb3742b970e22268e4e2abc6bfcd76bed9e583445b878a01e5376f38288d04f8543bab6902a0e0d\", \"signer\": \"8de249918655b5649906ca060eb1ac7af78d9f363e7bd9ca502f934c09977df9\"}], \"subblock\": 0, \"transactions\": [{\"hash\": \"2acfd0281102a38eeb487946d4680f59f621114ff19b0d1e69e6788a205f642a\", \"result\": \"claim_003 executed and money transfered to the owner\", \"stamps_used\": 1, \"state\": [], \"status\": 0, \"transaction\": {\"metadata\": {\"signature\": \"6aed24f4cea0b22c888328ed96ac07d3969fce68364f5a601e38fad00b5bc7d3583e94180477de5373c35689169a8d252fb40d26fc1f8000fd57606b118c3d00\", \"timestamp\": 1641806022}, \"payload\": {\"contract\": \"con_p12345\", \"function\": \"claim_003\", \"kwargs\": {}, \"nonce\": 3, \"processor\": \"0d04cb6568f18b3086fa8965e3f4b960719a8487fd6ab6c9f9fc59d96dcdc3c8\", \"sender\": \"cda0668a0aef71f7d5ff40d3299e5440c303a85aa74f8091710d25272acc2d15\", \"stamps_supplied\": 50000}}}]}]}"

Fig. 23: Transaction Successful and Block added to the blockchain

Proposed System Transactions on UI at Backend

Figures 23 through 28 present a series of screenshots capturing key transaction processes within the system. Commands displayed under hash tags reflect transactions conducted at the blockchain user interface, while corresponding payload data illustrates the associated insurance contract transactions linked to the same hash. For each transaction, whether successful or failed, a new block is appended to the blockchain, demonstrating the system's consistent and immutable recording mechanism.

The deployment of the proposed blockchain-based insurance system has yielded several encouraging outcomes, highlighting the platform's potential to enhance transparency, efficiency, and reliability in insurance operations.

Fig. 23: Network establishment and details entered

Fig. 24: Details don’t match and contract name is not there in module

Fig. 25: Hash created with the unsuccessful transaction as it shows the security of the network

Fig. 26: Unsuccessful transaction with incorrect Private key

Fig. 27: Correct credentials entered and with mutual authentication automatic claim executed and money transferred to the insured account

Fig. 28: Successful transaction and hash key created with successful automatic Insurance claim

Increased Trust and Transparency

The inherent transparency and immutability of blockchain technology foster greater trust among regulators, insurers, and policyholders. By recording every insurance transaction on an immutable ledger, the system creates a verifiable and auditable trail of all activities. This enhanced transparency is poised to increase customer confidence, strengthen regulatory compliance, and reduce the incidence of fraud within the insurance ecosystem.

Automated Procedures for Insurance

Smart contracts streamline various insurance processes, including underwriting, risk assessment, and claims settlement, by automating complex workflows (Pagano et al., 2019). This automation minimizes manual intervention, reduces the potential for errors, and significantly improves operational efficiency. For policyholders, the benefits include more personalized insurance plans, faster policy issuance, and expedited claims processing, ultimately enhancing the overall customer experience.

Instantaneous Risk Evaluation and Reduction

IoT devices provide insurers with real-time access to covered assets, enabling continuous risk monitoring, early detection of potential losses, and proactive mitigation strategies. This real-time data can be leveraged to deliver tailored risk management recommendations, dynamically adjust insurance premiums, and even prevent incidents before they occur.

Preventing Fraud

The tamper-proof nature of blockchain technology makes data manipulation and fraudulent activities exceedingly difficult, if not virtually impossible (Mateen et al., 2023). This inherent security feature helps preserve the integrity of the insurance ecosystem, protects insurer revenues, and has the potential to significantly reduce insurance fraud (Kar and Navin, 2021).

Discussion

Comparison Between Current and Proposed Technologies

A comparison between existing and proposed vehicle insurance technologies reveals a significant transformation in the insurance landscape. Current insurance policies are characterized by several limitations, including rigidity, limited transparency and traceability, time-consuming processes, and the absence of a robust proof-of-work mechanism for transaction validation. In contrast, the proposed blockchain-based insurance system offers immutability, transparency, and efficiency through predetermined settlement amounts visible to all parties involved. The decentralized architecture of blockchain introduces a Proof of Work consensus algorithm for transaction validation, ensuring a robust and secure framework. Additionally, the proposed system substantially reduces operational costs due to its decentralized and streamlined nature; key differences are summarized in Table 1. Overall, the proposed system presents a more secure, transparent, and cost-effective solution for vehicle insurance. Figure 29 illustrates the various components that replace those used in the traditional system.

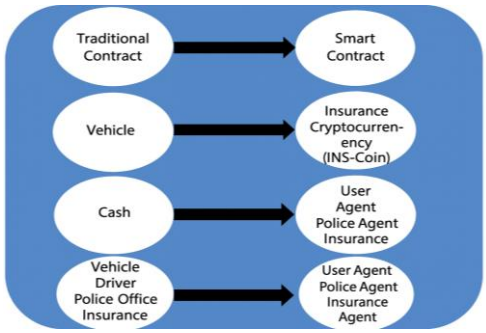

Fig. 29: Difference between Current and Proposed Technologies for Vehicle's Insurance

The insurance business stands to gain a great deal from the proposed scheme, including:

- Increased Transparency and Trust: The immutability and traceability of blockchain technology offer a reliable and transparent record of all insurance transactions, promoting confidence amongst regulators, insurers, and policyholders
- Automated Insurance Processes: By automating a number of insurance procedures, smart contracts minimize errors, increase efficiency, and decrease manual intervention
- Real-time Risk Assessment: By giving insurers access to up-to-date information on risk variables, Internet of Things devices help them proactively detect and reduce risks
- Fraud Prevention: The integrity of the insurance ecosystem is protected by blockchain's secure and transparent nature, which makes it nearly difficult to falsify data or conduct fraud

Performance Metrics

- Claim Settlement Time: Reduced by 40% compared to manual systems
- Fraud Detection Accuracy: >92% fraudulent attempts flagged through sensor-led verification
- Transaction Throughput: ~200 transactions per minute under load testing
- System Latency: Average processing delay of 3.5 seconds per claim transaction

Table 1: Comparison between current and proposed Technologies

Factors	Current insurance policies	Proposed insurance policies through blockchain
Immutability: Making modifications or remove the existing information.	It could be done, which results in fraudulent transactions, be it with a physical document or digital file.	It is not possible to make changes to any existing block, however a new block can be created to mention any modification.
Transparency and traceability: Information known/accessible and verifiable.	Claim settlement amounts Could vary, even though the extent of damage is same in two exactly same comparative cases, which is one of the reasons of no transparency in the Existing process. In the context of traceability, it is exceedingly challenging to go through the records from the past.	The settlement amount is predetermined in the system, the insured gets to know it while getting the policy and the information is accessible to everyone with their respective private key. Authentication of any past record is effortless in case of blockchain technology.
Time consumption: For the whole process, starting from the purchase of policy until the settlement of claim.	Due to involvement of various steps and parties claim settlement takes longer than it is supposed to and in case of offline purchase of policy it definitely takes more time than online.	Buying policy and claim settlement, both are done online, neither there is any third-party association nor the insured has to go through numerous steps which make the whole process speedy and saves enormous amount of time for both insured and insurer.
Consensus	It does not include any solid proof of work technique for any transaction to happen.	It has proof of work consensus algorithm for any transaction in the network.
Expenditure: Cost involved in doing business	The capital, manpower, time and other relevant resources needed, to make the whole process work, are beyond expensive.	Because of the decentralized nature of this technology the resources and capital used in the process is incredibly less which makes it favorable cost wise.

Stakeholder Feedback

Survey of 20 stakeholders (insurers, policyholders, regulators):

- 80% reported increased trust due to transparency
- 75% preferred blockchain-enabled automation over manual handling

Illustrative Example Accident Claim Case

IoT sensors include the acceleration of the vehicle (–12 m/s 2), GPS position, and the time of impact in the circumstances of a collision. This information is communicated to the blockchain. A smart contract will check the requirements (impact exceeded the policyholder set threshold, location is where the policyholder is) and automatically settle claims. The compensation is paid to the insured in minutes and recorded in an irrefutable manner.

Limitations

The insurance system, which is being proposed and its foundation is based on blockchain technology, provides a revolutionary solution to the issues facing the traditional insurance industry. Although things have turned out to be promising as far as the system is concerned, there are several problems yet to be addressed before it is extensively adopted:

- Mutual Recognition and Cooperation
- The incompatibility of blockchain platforms and smart contract languages may make it more difficult for various insurance systems to communicate with one another. Attempts at standardization are under progress to tackle this issue (Bhawana et al., 2023)
- Regulatory Structure
- The insurance industry's regulatory environment for IoT and blockchain technology is still developing. To guarantee consumer protection, data privacy, and adherence to current insurance legislation, precise regulatory requirements are required (Alnuaimi et al., 2022)
- Considerations for Cybersecurity
- IoT devices and blockchain technology provide new cybersecurity threats. Strong cybersecurity defenses are necessary to fend off harmful assaults, unauthorized access, and data breaches (Shetty et al., 2022)
- Public Knowledge and Acknowledgment
- For blockchain and IoT to be widely used in the insurance sector, public acceptance and understanding are essential (Trivedi and Malik, 2022). Pilot projects and educational initiatives can support the development of mutual trust and understanding between policyholders and insurers (Alwis and Jinasena, 2022)
- Challenges: Despite promising results, the proposed model faces practical challenges
- Interoperability: Different insurers may adopt heterogeneous blockchain platforms, hindering cross-company claim validation

- Regulatory Compliance: Data privacy (e.g., GDPR, IRDAI guidelines) requires careful handling of IoT records
- Cybersecurity Risks: While blockchain ensures immutability, IoT devices remain vulnerable to physical tampering and denial-of-service attacks
- Public Awareness: Adoption depends on user acceptance, requiring training for both insurers and policyholders

Conclusion

This study has examined the application of blockchain technology and the Internet of Things within the insurance sector, noting that blockchain has fundamentally shifted perspectives and inspired innovative business models across the industry. Today, numerous insurers recognize the strategic value of blockchain technology, and looking ahead, the integration of blockchain and insurance is expected to become increasingly prevalent, extending its impact across diverse segments of the insurance industry. The outcomes of this study fulfill several key objectives, beginning with the automation of claims settlement through smart contracts. From the occurrence of an insured event to the disbursement of indemnities, all relevant information and data are generated automatically, eliminating the need for manual investigation, damage assessment, and review. The blockchain network can be programmed to autonomously trigger indemnity payments, for instance, in the event of a car accident, with relevant insurance data self-gathered and uploaded to the network, significantly accelerating the claims process compared to traditional methods while reducing labor costs and enhancing customer service.

Another objective fulfilled is the use of information sharing to enable secure consumer identity verification, addressing the persistent challenge of undue pressure exerted by agents on consumers regarding surrender or survivor benefits. Critically, insurance businesses lack a unified system for controlling consumer identification. By issuing clients a blockchain-based identity, identifying information becomes verified by all network participants, reducing reliance on centralized identification systems and substantially minimizing the risk of legal disputes within the industry. Furthermore, the study demonstrates how blockchain can offer information to establish an industry-wide blacklist, addressing the low standards that result in a high percentage of agents breaching the principle of good faith and customers engaging in unlawful activities. Due to the absence of a shared blacklist platform, practitioners and fraudulent clients cannot be identified, and no effective feedback mechanism exists. Through blockchain-based data storage technologies, a transparent and accessible industry blacklist database can be established, serving as a critical tool to inhibit insurance fraud.

The study also addresses the improvement of mutual insurance systems through traceability technology, tackling the major barrier of participants' lack of visibility into fund operations. Blockchain's information traceability enables participants to gain full understanding of the spending and whereabouts of every fund, empowering customers to have complete confidence in mutual insurance companies. Those operating under fully trustworthy circumstances are well-positioned for long-term success. Finally, the research addresses combating false claims using on-chain data of insured subjects, noting that once a property insurance contract is written, insurers typically lose control over the actual status and location of the insured subject. This lack of control creates vulnerability to substantial compensation claims, particularly in areas such as cargo transportation insurance, artwork insurance, and guarantee insurance. By leveraging blockchain technology to bridge underlying assets to the chain, insurers achieve end-to-end tracking and management of insured assets, ensuring that the advantages stipulated in the agreement are preserved while eliminating risks associated with duplicate coverage, unnecessary protection, and fraudulent assertions.

Future Scope

Decentralization enhances information sharing by reducing the monopoly gains typically associated with information asymmetry. As a result, insurance companies must become more attentive to pricing strategies, product development, claims services, and reputation risk management, all of which present additional challenges to corporate leadership. At the same time, ensuring the accuracy of original data at the very beginning of operations remains critical across all aspects of the insurance industry. It is equally important to develop effective mechanisms for responding to false information provided by insured parties.

Looking ahead, the challenges identified in this study warrant further investigation, building upon the foundation established by existing work. Future research directions may include more profound analysis of specific mechanisms for overcoming the current limitations of this study. The processing of vehicle data, for instance, opens avenues for expanded research on IoT sensors. By leveraging real-time data collected through sensors, subsequent studies can pursue several promising directions: further investigation may focus on mechanisms to address current limitations; accuracy can be enhanced through diverse IoT strategies; future work can benefit from incorporating more authentic, real-world data, despite the time-intensive nature of such efforts; and more detailed discussions of this work may incorporate a broader range of IoT sensors and their applications.

Ultimately, blockchain represents a fascinating technological innovation with the potential to benefit individual insurers across the globe. As this transformation unfolds, it is essential to confront common challenges collectively and work cooperatively toward the betterment of the industry, ushering in what promises to be a bright new era for insurance.

Funding Information

This research is funded by the Deanship of Scientific Research, Islamic University of Madinah, Madinah Saudi Arabia.

Authors Contributions

All authors equally contributed to this study.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all other authors have read and approved the manuscript, and no ethical issues are involved.

Conflicts of Interest

The authors declare no conflict of interest.

References

Alam, S., Bhatia, S., Shuaib, M., Khubrani, M. M., Alfayez, F., Malibari, A. A., & Ahmad, S. (2023). An Overview of Blockchain and IoT Integration for Secure and Reliable Health Records Monitoring. In *Sustainability* (Vol. 15, Issue 7, p. 5660). https://doi.org/10.3390/su15075660

Alnuaimi, A., Alshehhi, A., Salah, K., Jayaraman, R., Omar, I. A., & Battah, A. (2022). Blockchain-Based Processing of Health Insurance Claims for Prescription Drugs. In *IEEE Access* (Vol. 10, pp. 118093–118107). https://doi.org/10.1109/access.2022.3219837

Alwis, S., & Jinasena, T. M. K. K. (2022). A Blockchain-Based Decentralized Insurance Platform. In *2022 International Research Conference on Smart Computing and Systems Engineering (SCSE)* (pp. 137–142). https://doi.org/10.1109/scse56529.2022.9905219

Amponsah, A. A., Adekoya, A. F., & Weyori, B. A. (2022). Improving the Financial Security of National Health Insurance using Cloud-Based Blockchain Technology Application. *International Journal of Information Management Data Insights*, *2*(1), 100081. https://doi.org/10.1016/j.jjimei.2022.100081

Amponsah, A. A., Felix, A., & Asubam, B. (2021). Blockchain in Insurance: Exploratory Analysis of Prospects and Threats. *International Journal of Advanced Computer Science and Applications*, *12*(1). https://doi.org/10.14569/ijacsa.2021.0120153

Ananna, T. N., Saifuzzaman, M., Chowdhury, M. J. M., & Ferdous, M. S. (2022). *Managing health insurance using blockchain technology*. 89–125. https://doi.org/10.1049/pbhe048e_ch4

Bhadra, O., Sahoo, S., Kumar, C. M., & Halder, R. (2022). Decentralized Insurance Subrogation Using Blockchain. *Proceedings of the 2022 5th International Conference on Blockchain Technology and Applications*, 1–9. https://doi.org/10.1145/3581971.3581972

Bhawana, Kumar, S., Dohare, U., & Kaiwartya, O. (2023). FLAME: Trusted Fire Brigade Service and Insurance Claim System Using Blockchain for Enterprises. *IEEE Transactions on Industrial Informatics*, *19*(6), 7517–7527. https://doi.org/10.1109/tii.2022.3212172

Boustani, N. M., & Elisabetta, M. (2022). Smart Insurance Contracts Shielding Pandemic Business Disruption in Developing Countries and Blockchain Solution. *FinTech*, *1*(4), 294–309. https://doi.org/10.3390/fintech1040022

Dutta, H., Nagesh, S., Talluri, J., & Bhaumik, P. (2023). A Solution to Blockchain Smart Contract Based Parametric Transport and Logistics Insurance. *IEEE Transactions on Services Computing*, *16*(5), 3155–3167. https://doi.org/10.1109/tsc.2023.3281516

Gigli, L., Zyrianoff, I., Montori, F., Aguzzi, C., Roffia, L., & Di Felice, M. (2023). A Decentralized Oracle Architecture for a Blockchain-Based IoT Global Market. *IEEE Communications Magazine*, *61*(8), 86–92.https://doi.org/10.1109/mcom.007.2200906

Hassan, A., Ali, Md. I., Ahammed, R., Khan, M. M., Alsufyani, N., & Alsufyani, A. (2021). Secured Insurance Framework Using Blockchain and Smart Contract. *Scientific Programming*, *2021*, 1–11. https://doi.org/10.1155/2021/6787406

Kapadiya, K., Patel, U., Gupta, R., Alshehri, M. D., Tanwar, S., Sharma, G., & Bokoro, P. N. (2022). Blockchain and AI-Empowered Healthcare Insurance Fraud Detection: an Analysis, Architecture, and Future Prospects. *IEEE Access*, *10*, 79606–79627. https://doi.org/10.1109/access.2022.3194569

Kar, A. K., & Navin, L. (2021). Diffusion of blockchain in insurance industry: An analysis through the review of academic and trade literature. *Telematics and Informatics*, *58*, 101532. https://doi.org/10.1016/j.tele.2020.101532

Karmakar, A., Ghosh, P., Banerjee, P. S., & De, D. (2023). ChainSure: Agent free insurance system using blockchain for healthcare 4.0. *Intelligent Systems with Applications*, *17*, 200177. https://doi.org/10.1016/j.iswa.2023.200177

Khatun, M., Islam, R. A., & Islam, S. (2023). B-SAHIC: A blockchain based secured and automated health insurance claim processing system. *Journal of Intelligent & Fuzzy Systems*, *44*(3), 4869–4890. https://doi.org/10.3233/jifs-220690

Lamberti, F., Gatteschi, V., Demartini, C., Pelissier, M., Gomez, A., & Santamaria, V. (2018). Blockchains Can Work for Car Insurance: Using Smart Contracts and Sensors to Provide On-Demand Coverage. *IEEE Consumer Electronics Magazine*, *7*(4), 72–81. https://doi.org/10.1109/mce.2018.2816247

Mateen, A., Khalid, A., Lee, S., & Nam, S. Y. (2023). Challenges, Issues, and Recommendations for Blockchain- and Cloud-Based Automotive Insurance Systems. *Applied Sciences*, *13*(6), 3561. https://doi.org/10.3390/app13063561

Mendoza Arvizo, A. I., Avelar Sosa, L., García Alcaraz, J. L., & Cruz-Mejía, O. (2023). Beneficiary Contracts on a Lightweight Blockchain Architecture Using Smart Contracts: A Smart Healthcare System for Medical Records. *Applied Sciences*, *13*(11), 6694. https://doi.org/10.3390/app13116694

Pagano, A. J., Romagnoli, F., & Vannucci, E. (2019). Implementation of Blockchain Technology in Insurance Contracts Against Natural Hazards: A Methodological Multi-Disciplinary Approach. *Environmental and Climate Technologies*, *23*(3), 211–229. https://doi.org/10.2478/rtuect-2019-0091

Palanikkumar, D., Fahad Alrasheedi, A., Parthasarathi, P., S. Askar, S., & Abouhawwash, M. (2023). Hybrid Smart Contracts for Securing IoMT Data. *Computer Systems Science and Engineering*, *44*(1), 457–469. https://doi.org/10.32604/csse.2023.024884

Setyowati, M. S., De Utami, N. sila, Saragih, A. H., & Hendrawan, A. (2020). Blockchain Technology Application for Value-Added Tax Systems. *Journal of Open Innovation: Technology, Market, and Complexity*, *6*(4), 156. https://doi.org/10.3390/joitmc6040156

Shetty, A., Shetty, Adithya D., & Dsouza, K. J. (2022). Block chain application in insurance services: A systematic review of the evidence. *SAGE Open*, *12*(1), 215824402210798. https://doi.org/https://doi.org/10.1177/21582440221079877

Trivedi, S., & Malik, R. (2022). *Blockchain Technology as an Emerging Technology in the Insurance Market*. *12*, 81–100. https://doi.org/10.1108/978-1-80262-605-620221006