

bradscholars

Blockchain-based secure privacy-preserving vehicle accident and insurance registration

Item Type	Article
Authors	Yadav, A.S.;Vincent, Charles;Pandey, D.K.;Gupta, S.;Gherman, T.;Kushwaha, D.S.
Citation	Yadav AS, Charles V, Pandey DK et al (2023) Blockchain-based secure privacy-preserving vehicle accident and insurance registration. Expert Systems with Applications. 230: 120651.
DOI	https://doi.org/10.1016/j.eswa.2023.120651
Publisher	Elsevier
Rights	© 2023 Elsevier Ltd. All rights reserved. Reproduced in accordance with the publisher's self-archiving policy. This manuscript version is made available under the CC-BY-NC-ND 4.0 license.
Download date	2026-06-08 18:05:09
Link to Item	http://hdl.handle.net/10454/19459

Blockchain-based Secure Privacy-Preserving Vehicle Accident and Insurance Registration

Amrendra Singh Yadav

Department of Computer Science and Engineering, Atal Bihari Vajpayee Indian Institute of Information Technology and Management, Gwalior, India

Email: asy@iiitm.ac.in

ORCID: <https://orcid.org/0000-0003-0241-3661>

Vincent Charles

School of Management, University of Bradford, Bradford, United Kingdom

Email: c.vincent3@bradford.ac.uk

ORCID: <https://orcid.org/0000-0001-8943-5681>

Dharen Kumar Pandey

P.G. Department of Commerce, Magadh University, Bodhgaya, Bihar, India

Email: dharenp@gmail.com

ORCID: <https://orcid.org/0000-0002-0030-1781>

Somya Gupta

Motilal Nehru National Institute of Technology Allahabad, Uttar Pradesh, India

Email: 15somyagupta@gmail.com

ORCID: <https://orcid.org/0000-0002-8853-5565>

Tatiana Gherman

Faculty of Business and Law, University of Northampton, Northampton, United Kingdom

Email: tatiana.gherman@northampton.ac.uk

ORCID: <https://orcid.org/0000-0003-2989-8427>

Dharmender Singh Kushwaha

Motilal Nehru National Institute of Technology Allahabad, Uttar Pradesh, India

Email: dsk@mnnit.ac.in

ORCID: <https://orcid.org/0000-0003-3067-6928>

Blockchain-based Secure Privacy-Preserving Vehicle Accident and Insurance Registration

Abstract

Insurance claims processing involves multiple entities and data sources, necessitating communication between human agents. Consequently, vehicle insurance claims have traditionally required significant human effort and time. Daily vehicle-related transactions, including those managed by transportation authorities, pose challenges for tracking. Centralised systems have been utilised for national solutions, but trust management, transparency, and access control issues arise. There is potential for further integration of vehicle-related transactions. This article proposes a blockchain framework for vehicle insurance to streamline the reporting of accidents and filing of insurance claims. Blockchain-based automation platforms can enhance the scale and response time of claims processing, providing users with control over additional transactions, inspection, and insurance. For experimental purposes, a blockchain was created using Hyperledger Fabric to store information about vehicles, owners, and insurance. Efficient querying of this blockchain requires specific participants, assets, and transactions. The consensus algorithm can identify invalid claims if a transaction request contains an error. By deploying blockchain technology and smart contracts, this architecture has the potential to address trust and security concerns associated with traditional insurance policies and claims.

Keywords: Vehicle Insurance; Blockchain Technology; Hyperledger Fabric; Smart Contract; Peer-to-Peer; Accident.

1. Introduction

The discipline of computer science is witnessing the emergence of a new technology known as a blockchain, which has a variety of potential uses and applications (for recent reviews and applications, see e.g., Charles *et al.* (2023) and Emrouznejad and Charles (2022)). Blockchain is a public, general ledger that records transactions between two parties in a suitable, safe, and transparently auditable manner. Figure 1 depicts some of the cryptography used to link and back up the ever-growing list of records that make up the blockchain's blocks. A peer-to-peer network is typically implemented when blockchain technology is utilised in a distributed ledger. Every peer adheres to a communication protocol between nodes in the network and a validation procedure for blocks (Nakamoto, 2009). Once information is added to a block, it cannot be modified without the consent of the majority of network users and the medication of all subsequent blocks in the blockchain. Although the entries in a blockchain can be changed, the technology underlying the blockchain is exceptionally safe and functions as a distributed computing system that is highly error tolerant.

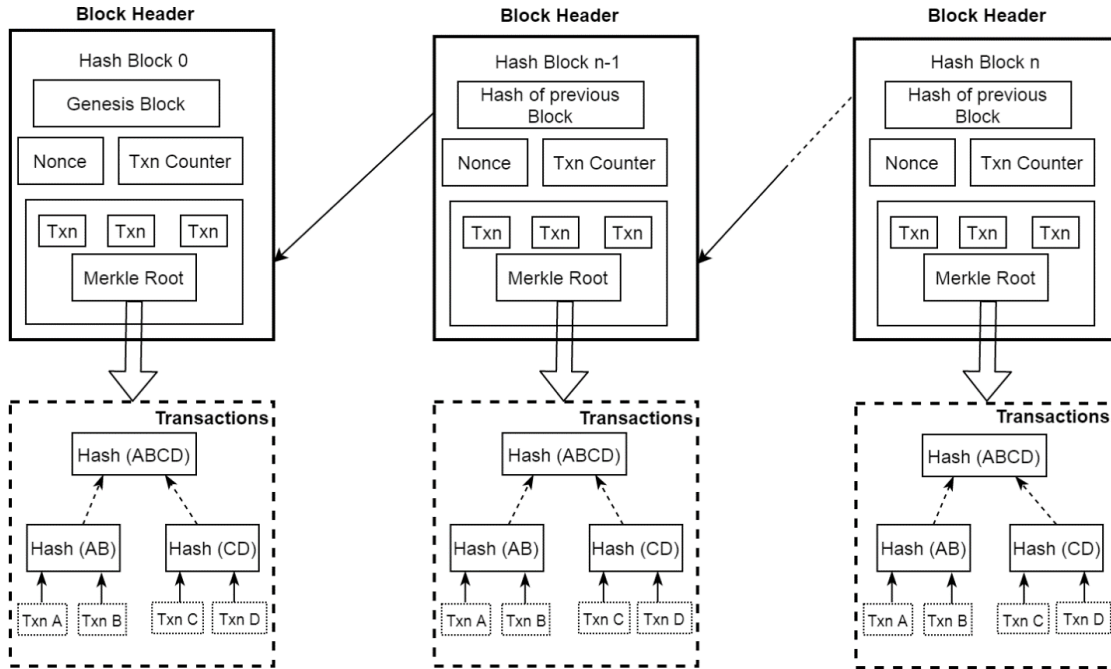


Figure 1. Blockchain Structure Consisting of a Sequence of Blocks.

Due to a lack of understanding, there are several unrealisable implementations. Blockchain, like other technological tools, has business benefits. Even though there is a lot of theoretical information about blockchain technology and its uses, it has not been put into practice nearly as much as it has been written about.

The insurance industry is transitioning to digitalization (Gupta *et al.*, 2022), utilising blockchain technology to make vehicles, cybersecurity, and connected cars scalable and auditable. This has allowed insurance companies and other parties to settle claims efficiently. Blockchain technology can be used to help with health, business, and car insurance matters.

An insurance policy represents an agreement under which a person or entity receives financial assistance or reimbursement from an insurance company in the event of a loss. Indeed, insurance is one of the most widely used forms of security in the world. It is estimated that the global insurance industry will be worth approximately \$8.4 trillion US dollars by 2026 (Statista, 2022). There are various types of health, business, and auto insurance coverage, and industrialised nations throughout the world have implemented many of these policies. National policies have established national health coverage plans in large portions of America, Europe, Japan, Australia, and Canada. Despite the prevalence of insurance plans, settlement processing is not always effortless or error-free. Insurance companies frequently misrepresent terms and conditions to avoid paying the insured, and fraudulent claims can cause issues for insurance firms. Traditional contractual procedures are often flawed and contain ambiguities, which can be exploited by both insurers and policyholders. Smart contracts on the blockchain can address these issues by clarifying the law and reducing the need for trust and financial risk in agreements. This can make insurance contracts more transparent, efficient, and fraud-free.

Both insurers and insured individuals often take advantage of these flaws in insurance contracts. However, as mentioned, with the introduction of smart contracts on the blockchain, the need for trust and financial risk in these agreements can be eliminated. This study proposes a conceptual

framework for using blockchain and smart contracts in the insurance industry, with the goal of ensuring safe and fraud-free transactions. The framework uses blockchain technology to manage various aspects of insurance, including customer registration, insurance claim submission, claim approval by the police, settlement of insurance company refunds, and application closure. By leveraging blockchain technology, this framework can help strengthen the entire insurance industry.

In a nutshell, in this study, the potential of blockchain and smart contracts is demonstrated by applying them to the insurance industry. The main objective is to create a conceptual framework that ensures secure transactions and eliminates insurance fraud. This framework leverages blockchain technology to manage customer registration, policy issuance, and refund settlements, resulting in a stronger insurance system. Furthermore, the consensus mechanism can be employed to verify blockchain entries.

Vehicle Accident Register Blockchain (VARB) uses blockchain to reduce the likelihood of fraud by time-stamping all relevant events and claims and providing a fast response in an emergency. Faster reimbursement from insurance companies, which requires less effort to process accident claims, is the major motivation for the proposed approach.

The proposed work implements a novel use case, which is a blockchain-based solution for a vehicle insurance network built on a Hyperledger Fabric network. It elaborates on the design specifics and the advantages of utilising such a solution. In section 2, we conduct a literature review on the applications of blockchain technology in the insurance sector. This review looks at some of the most prominent applications of blockchain technology in various domains (Dhieb *et al.*, 2020).

The proposed Hyperledger-based VARB makes use of various assets, participants, and transactions. We secure all transactions by using the core underlying principles of blockchain. All the data are stored in a ledger. The participants are the vehicle owner, police, a witness, the owner's close relative, the insurer, the insurance adjuster, and the repair shop. The assets are the vehicles and the insurance. Transactions contain information about reporting the vehicle, the loss incurred, and the accident details. The insurance surveyor has the right to modify and adjust the insurance amount based on the vehicle's damage. The actual owner claims the vehicle insurance, and based on that, the vehicle is repaired at the garage. If the owner dies in such an accident, the insurance is claimed by a close relative. Each asset, participant, and transaction have their unique identifier, and these are time-stamped to secure and protect them from replay attack.

1.1 Background

In this subsection, we examine the history of the underlying technology behind the blockchain and the insurance system.

1.1.1 Hyperledger Fabric Platform Development

To assess the overall performance of the platform, a Hyperledger Fabric platform instance is set up for experimentation. The Hyperledger Fabric Distributed Ledger Technology (DLT) platform is the first major private DLT system born out of the Hyperledger ecosystem. To ensure that a variety of governmental agencies and corporate organisations can benefit from a DLT-based system in various use cases, it has been created with a heavy focus on privacy protection. This useful feature allows the Fabric to manage numerous ledgers within its DLT systems, despite the fact that each domain consists of only one ledger. The Fabric's modular design and pluggable functionalities are two more significant strengths of the platform. In addition, the consensus mechanism is pluggable, which means several types of consensus algorithms can be utilised

depending on the circumstances. Currently, Fabric is compatible with SOLO and Kafka, and an SBFT (Simplified Byzantine Fault Tolerance) method will be made available very soon. Hyperledger Fabric does not support a decentralised network (Benhamouda *et al.*, 2019). Most of the time, it is controlled by a single entity or a group of entities with shared responsibility.

Hyperledger Fabric has some significant differentiating capabilities over other well-known distributed ledger or blockchain platforms (Manevich *et al.*, 2019). It improves performance while preserving privacy. Hyperledger Fabric is one of the first distributed ledger platforms to allow users to build Smart Contracts (SCs) using programming languages other than Domain-Specific Languages (DSLs), such as Go, JavaScript, and Node.js (DSL). From this, we can deduce that most companies already possess the skill set necessary to build SCs (Kocsis *et al.*, 2017), and there is no longer a need for additional training to learn a new language or DSL. The following elements are included in the construction of Fabric:

- When it comes to transactions, when an ordering service establishes consensus, then it broadcasts blocks to the other peers in the network.
- A provider of membership services whose primary mission is to bring together various organisations. Cryptographic identities are used within the network.
- The blocks that are provided as an output by an ordering service are distributed by other peers via a peer-to-peer gossip service.
- Containers are the environments in which SCs carry out their operations. They can be programmed in any standard programming language, but they do not have direct access to the ledger state.
- An endorsement and validation policy can be configured separately for each application.

Hyperledger Fabric is an open-source framework designed for building private blockchain business applications, with the identities and roles of members known to one another. Its backend consists of a fabric network, while its frontend is an application on the client-side. The architecture of Hyperledger Fabric is modular, as illustrated in Figure 2.

Hyperledger Composer is a collection of Javascript-based tools and scripts that simplify the process of setting up Hyperledger Fabric networks. Using these tools, we can create a Business Network Archive (BNA) for our network. Composer includes several components such as:

- a. Business Network Archive (BNA)
- b. Composer Playground
- c. Composer REST Server

a. Business Network Archive: Composer enables the bundling of various files into a single package, creating an archive that can be deployed on a Fabric network. To create this archive, we need the following:

- *Network Model:* A list of the resources available on the network, such as assets, participants, and transactions.
- *Business Logic:* Logic for the transaction functions.

- *Access Control Limitations*: Different rules that define the rights of each participant in the network. This includes deciding which assets participants can control.
- *Query File (optional)*: A set of questions that can be asked of the network, similar to SQL queries.

b. Composer Playground: This is a user interface based on the web that can be used to model and test a business network. It is great for creating simple Proofs of Concept, as it simulates the blockchain network using the browser’s local storage. If we are running a local Fabric runtime and a network has been set up, the playground can also be used to connect to that network. In this case, the playground is not a simulation of the network. Instead, it talks directly to the Fabric runtime on the local machine.

c. Composer REST Server: This tool allows us to create a REST API server based on our business network definition. Client applications can use this API, enabling us to add apps that do not use blockchain to the network.

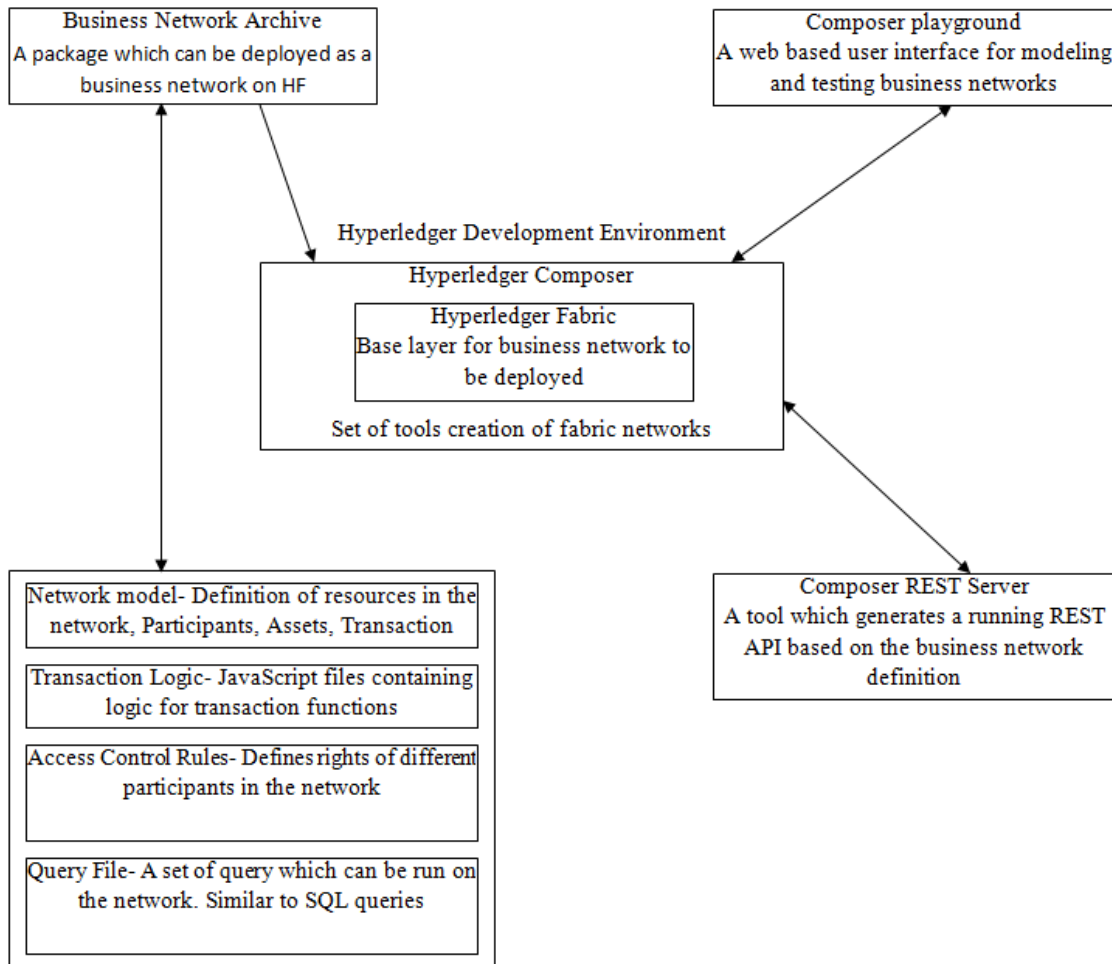


Figure 2. Development Environment Overview for a Hyperledger Fabric Network.

This study utilises the Linux-Ubuntu operating system to install and run the entire Hyperledger Fabric deployment. Each component of the Hyperledger Fabric is initially started as a separate Docker container. The components include peers, the Ordering Service (OS), and the Certificate Authority (CA). It should be noted that the execution of transactions and the maintenance of each participant group's ledger is the responsibility of a peer that that participant group manages; an operating system provides services such as broadcasting messages and guaranteeing the delivery of messages, etc.; and a certification authority provides certificate services to participants in a blockchain (Nunez Mencias *et al.*, 2018).

1.1.2 Sequence diagram using Hyperledger chain code

A peer-to-peer network of computers is typically utilised in blockchain to verify every transaction. A blockchain is a data structure that generates and distributes a distributed ledger of transactions across networks of computers. Blockchains are also known as digital ledgers. Any user can conduct a transaction and immediately check that it was completed successfully without fear of being monitored by a centralised authority. The primary objective of this piece of software is to demonstrate how blockchain technology can be used to streamline insurance transactions in the context of a real-world scenario involving an accident. This programme can only be utilised in situations where each vehicle has a unique identity. The survey number serves as the primary key that identifies each insurance in a unique way. We have two peers responsible for maintaining their independent copy of the ledger. The ledger's two components are a world state and a blockchain. In comparison to other blockchain platforms, the fundamental architecture of Hyperledger is quite distinctive (Nunez Mencias *et al.*, 2018). It adheres to the execute-order-validate model, as opposed to other blockchain platforms, which comply with the order execute-to-validate model (see Figure 3).

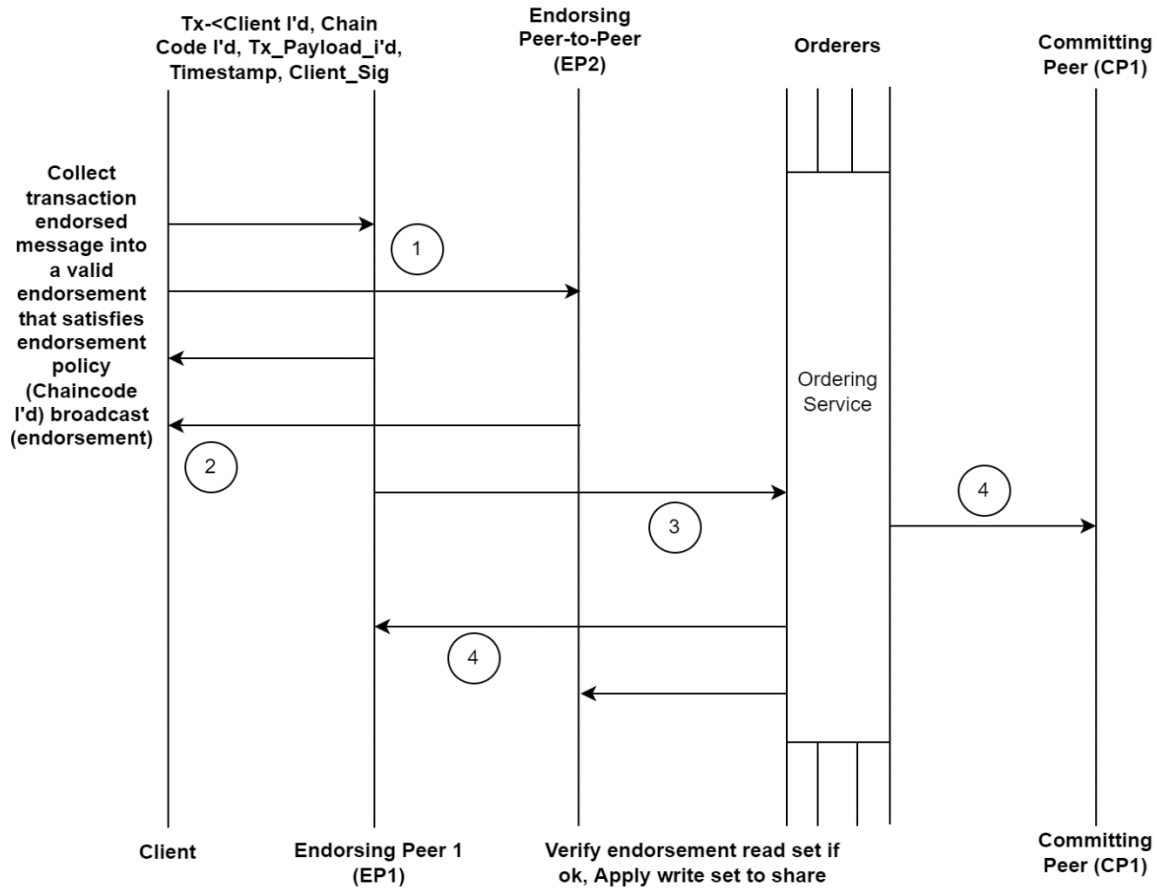


Figure 3. Sequence of Steps Involved in the Chain Code.

The execution, ordering, and validation phases of Hyperledger fabric are as follows:

- *Execution:* During the execution stage of Hyperledger, the client application communicates its proposal to a group of peers. They achieve this by invoking a SC to update the ledger and then endorsing the outcomes. The client application receives the proposed update of the ledger from the peers who endorse it.
- *Ordering:* In the ordering phase, the transaction that contains the endorsed transaction is submitted by the client, and the ordering service node responds to its proposal. The ordering service node makes blocks of transactions, which are then sent to all the peers for final validation.
- *Validation:* In the validation phase, each peer's distributed blocks are validated independently and deterministically so that the ledger remains uniform. Specifically, every transaction is validated by every peer in the channel by ensuring that many peers have endorsed the transaction and that the endorsements are the same. The peer flags invalid transactions as invalid, at which point these are stored in the immutable block; nonetheless, the global state of the ledger does not get altered.

- *End-User*: In our scenario, end-users are the participants, *i.e.*, the owner, police, third person, insurer, and insurance adjuster. Every participant has some authorised rules under which they can perform particular transactions.
- *Peer*: The peer maintains the up-to-date copy of the ledger. After receiving a transaction proposal from the participant, an endorsing peer executes the transaction. At this point, the peer checks to see whether the transaction is valid and does not make any permanent changes to the ledger. For example, a peer may check whether or not the current owner specified in the insurance is a valid owner. After executing the transaction, a peer returns the result to the web server. Only after receiving a block from the ordering service does a peer make any permanent changes to the ledger. Here also, some transactions may not have enough endorsements. In the latter case, the peer adds the block to its blockchain but marks the transaction as invalid and does not apply it.
- *Ordering Node*: After receiving endorsements from the required number of peers for a given transaction, the web server passes the transaction to the orderer. The orderer gathers these transactions from many web servers, packages them into blocks, and broadcasts them to their peers.

1.1.3 Smart Contract

An SC is an agreement between two parties that is enforced by the blockchain-based implementation. It is executed after reading through all of the blocks in the chain. Because the blocks are infallible, the accuracy of the transaction can be guaranteed since it uses a distributed ledger to store contracts (Hewa *et al.*, 2021). In the real world, contracts are referred to as SCs. The sole distinction is that these are entirely composed of digital content. An SC is a computer programme stored within a blockchain. These are both immutable and distributed. The immutability property ensures that once an SC is created, it cannot be changed, eliminating the risk of tampering.

The distributed transactions allow everyone on the network to validate the SC output. A computer system, such as a distributed ledger that is appropriate for the task, can automatically carry out the terms of an intelligent contract. A state machine is a piece of logic that can be executed, producing new facts that are then added to the ledger (Wang *et al.*, 2019). In business operations, the collaborating parties must trust each other and ensure that they understand the transaction details. Every blockchain is supported by a business model. SC is the logic that can be executed and is responsible for generating new facts that are then added to the ledger. Before we describe our SC, we must first define the business logic underlying our VARB. For a software developer, SC is the main component of Hyperledger Fabric, which contains the core code.

SC has a wide range of potential applications. SC can assist manufacturers in the process of making callbacks for each vehicle. This information can be displayed to the driver via a user interface in the vehicle. The owner of the vehicle or the driver can respond with decisions. Because the blockchain would record every action, it would be impossible to alter the data. The interaction and reactions cannot be denied. The automatic management of SC is one of the most important characteristics of blockchain networks (Khan *et al.*, 2021). To the extent that blockchains are utilised to record transactions, users can develop contracts that will cause the network depicted in Figure 4 to execute trades.

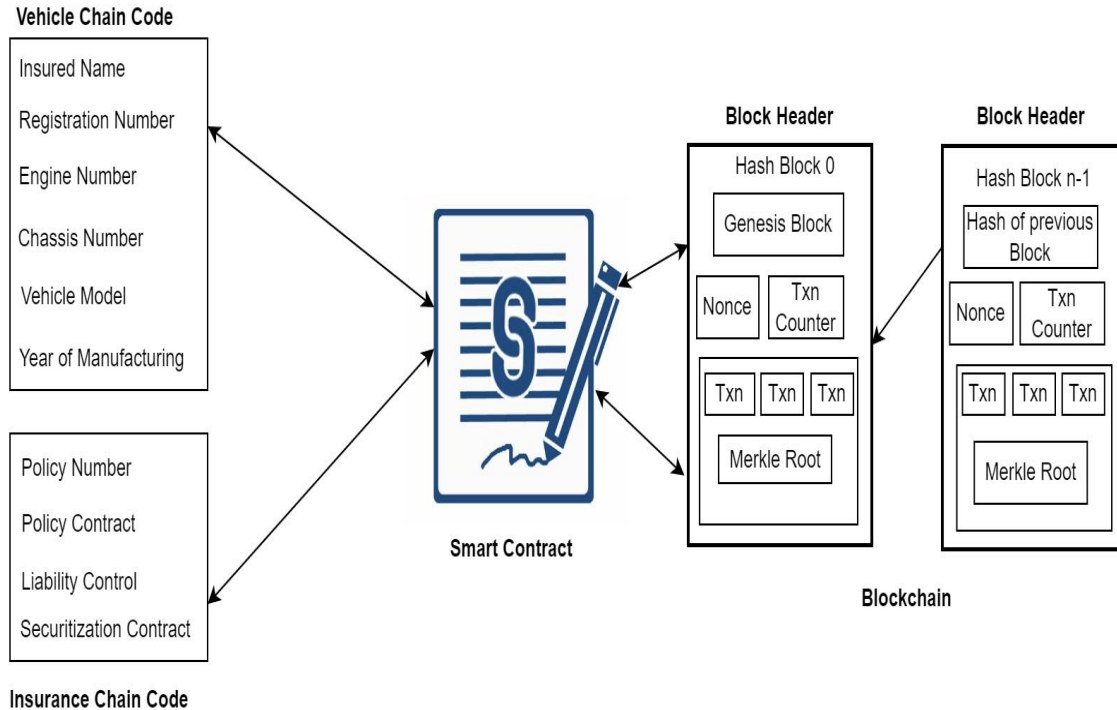


Figure 4. Working of a Smart Contract Model.

The use of blockchain technology ensures that each participant adheres to the collaborative insurance model. To improve the transparency of insurance transactions, collaborative entities that cannot be trusted must follow the non-repudiation principle. To reduce administrative and operational costs, as well as to automate and speed up business operations in the insurance industry from the time, an individual insured signs up for coverage to the time a claim is handled.

This article presents a consensus process that is both faster and more efficient than the Bitcoin network, as well as a blockchain-based automobile insurance system that requires only a small number of messages to function properly.

In line with the above, the specific research objectives addressed in the present work are as follows:

1. To propose an insurance solution based on smart contracts and blockchain technology.
2. To identify the benefits of leveraging blockchain technology and smart contracts to provide peer-to-peer collaborative insurance.
3. To evaluate how customers depend on one another to satisfy insurance requirements, eliminating a centralized authority and implementing an insurance system based on blockchain technology. The novelty of this work stems from the fact that none of the currently available digital insurance solutions can cover the entire insurance business process.
4. To identify the operational concepts of the proposed vehicle insurance-based blockchain framework that is self-enforcing and based on voting processes and external oracles.
5. To assess how performance and scalability can be enhanced as the number of insurance claims and insurers grows.

The remaining sections of the paper are laid out as follows. The literature survey is discussed in the following Section 2. Section 3 introduces the proposed vehicle insurance-based blockchain framework. The proposed algorithm is discussed in Section 4. Section 5 shows the results of the

analysis and experiments. Subsequently, Section 6 discusses security and privacy. How the Insurance companies tend to gain by adopting this proposed research has been discussed in section 7. Finally, Section 8 concludes the article by suggesting potential future directions.

2. Literature Review

Several countries have moved toward creating a distributed, automated, integrated system responsible for maintaining and controlling vehicle data. A design like this that is integrated offers benefits to several different parties, including the government, vehicle owners, insurance firms, potential vehicle buyers, and vehicle parties that are looking for correct information (Gera *et al.*, 2020). Cyberattacks are a significant issue that many insurance companies face. In addition, malfunctioning smart devices transfer incorrect information to other devices, causing the insurer to receive inaccurate data (Bhawana *et al.*, 2023). Using blockchain as a system service to design a distributed platform to support transaction execution in the insurance process is a central concept reported in (Raikwar *et al.*, 2018).

Many efforts have been made to use blockchain to solve vehicle insurance registration problems. Praticcò *et al.* (2021) proposed a mobile application platform and a vehicle-mounted electronic device. The platform lets the driver change their insurance status in real-time. Each change and picture are recorded in the ledger of an SC to prove that the changes were made and to keep track of the vehicle's status.

Bader *et al.* (2018) proposed an SC-based ecosystem for a transparent and straightforward vehicle insurance procedure. Instead of completely replacing existing procedures, the software they offer supports them, allowing for significant cost savings. This was made feasible by eliminating the need for manual insurance claims inspections, which tamper-proof automobile sensors would now carry out. Authors proposed a trust value-based mechanism that reduces message exchange between peers when compared to Proof-of-Work (PoW), Proof-of-e (PoS), and Distributed Proof-of-Stake (DPoS) consensus mechanisms. However, the parties involved can also undertake traditional operations at any time, allowing them to strike a balance between the process's reliability and cost-effectiveness. Thus, the software demonstrates how SCs can support insurers without introducing new risks.

Oham *et al.* (2018) came up with a Framework for Auto-Insurance Claims and Adjudication (B-FICA) for Connected and Automated Vehicles by using blockchain technology (CAVs). This framework stores both the sensors' data and the interactions between entities that can be checked. To communicate information on a need-to-know basis, B-FICA uses a legal blockchain with two partitions. It provides proof of execution, appropriateness, and dependability by utilising transactions that have been digitally signed. In addition, it employs a dynamic and uncomplicated consensus and validation mechanism to prevent tampering with the evidence. According to the findings of the qualitative evaluation, B-FICA is resistant to many security attacks from possible attackers who could compromise the system's security.

Teambrella is an insurance platform company whereby a claimant team co-insures the claims instead of a centralised insurance company. Teambrella uses SCs and blockchain to execute insurance payments. Members of a Teambrella group are provided with a SC, which they use to vote and, as a result, use some consensus algorithm to execute payment for each claim transparently (Shetty *et al.*, 2022). According to Dorri *et al.* (2017), blockchain has prevented fraudulent intelligence data in insurance systems. Syed *et al.* (2020) proposed assisting decision-makers by demonstrating the capabilities of blockchain technology. Singh and Kim (2018) proposed an approach for evaluating auto insurance payment systems.

The insurance industry has started utilising blockchain to turn different parts of insurance policies into smart contracts, which can automate insurance operations (Kshetri, 2021). In Guo and Yu (2022), the authors showed a file system that works worldwide and an auto insurance system that uses blockchain to automate making and paying for claims. Furthermore, the authors focus on the security of blockchain in this article. In Reebadiya *et al.* (2021), a plan was proposed for an auto insurance claims system based on blockchain, which would allow vehicles to share information using sensors. Meanwhile, Nizamuddin and Abugabah (2021) suggested tracking vehicle insurance information using blockchain to help settle disagreements. Smart contracts were proposed to automate a blockchain-based system for auto insurance. The authors proposed a decentralized IPFS and blockchain-based framework for the auto insurance sector that regulates and automates automobile insurance claims. In Oham *et al.* (2018), a transportation insurance prototype that combines blockchain and IoT was presented. It enables drivers to share real-time information via GPS communication. The authors created an automatic service for filing medical insurance claims using blockchain and smart contracts to help control risks and prevent money laundering. With two-sided verification for sensor data and entity interactions, the authors proposed a BlockChain-based Framework for Auto-insurance Claims and Adjudication (B-FICA) for CAVs. Nanda *et al.* (2023) proposed a decentralised car insurance system that uses machine learning and distributed ledger technology. To address scalability and efficiency concerns, Yadav *et al.* (2022a, 2022b, 2023) suggested using sidechains.

In Pawar and Sachdeva (2023), the authors proposed a low-energy consumption using blockchain-based system for sharing medical insurance information among hospitals, patients, and insurance companies. Similarly, Iyer *et al.* (2021) suggested a decentralised peer-to-peer crop insurance system for farmers to cover the risk of too much rain, while Salem *et al.* (2021) proposed a blockchain-based smart contract framework for the drought insurance system. In Xiong *et al.* (2020), the authors proposed a crop insurance system that uses blockchain to ensure timely payment to insured farmers, and Parlak (2023) presented a blockchain-based framework for automating insurance policy, claim, and payment processes using smart contracts.

Many traditional businesses, such as insurance companies, have recently evolved. The conventional algorithm for managing insurance companies has numerous flaws. Established insurance companies may have treated high-risk and low-risk customers equally. Traditional companies have few tools for categorizing users based on their risks.

Due to the various research gaps found in the reviewed literature, there is a need for a framework capable of handling vehicle insurance transactions that are efficient, quick, fraud-free, tamper-proof, and dependable. The current methods for obtaining auto insurance take too long to complete transactions and do not lay a solid enough foundation. The related consensus methods send out a large number of messages, increasing the amount of overhead for each transaction.

3. Proposed Vehicle Insurance-based Blockchain Framework

It has been suggested that a unique vehicle insurance management system may be developed to handle matters about vehicle insurance. The proposed blockchain based framework illustrated in figure 5 has been described in three subsections. Section 3.1 elaborates on the vehicle insurance framework without blockchain. Section 3.2 demonstrates the proposed framework for vehicle insurance-based blockchain framework. Section 3.3 describes the proposed framework's network architecture. Participants in the proposed blockchain network include individual drivers/owners, regional legal authorities, insurance companies, service technicians, auto manufacturing companies, and the government regional transport office.

3.1 Vehicle Insurance Framework without Blockchain

In many countries, vehicle insurance is mandatory. Each driver of the vehicle must provide proof of insured property along with an insurance copy upon request. When pulled over by the police, motorists are required to produce evidence that they are adequately insured. This is also required when purchasing or leasing a vehicle, registering a vehicle, or renewing license plate stickers. In these scenarios, the drivers negotiate individually with each party. An example of a transaction is when a person buys a new car and signs an insurance policy with the insurance company and then submits the paperwork from the car dealer for the approval and licensing of the vehicle.

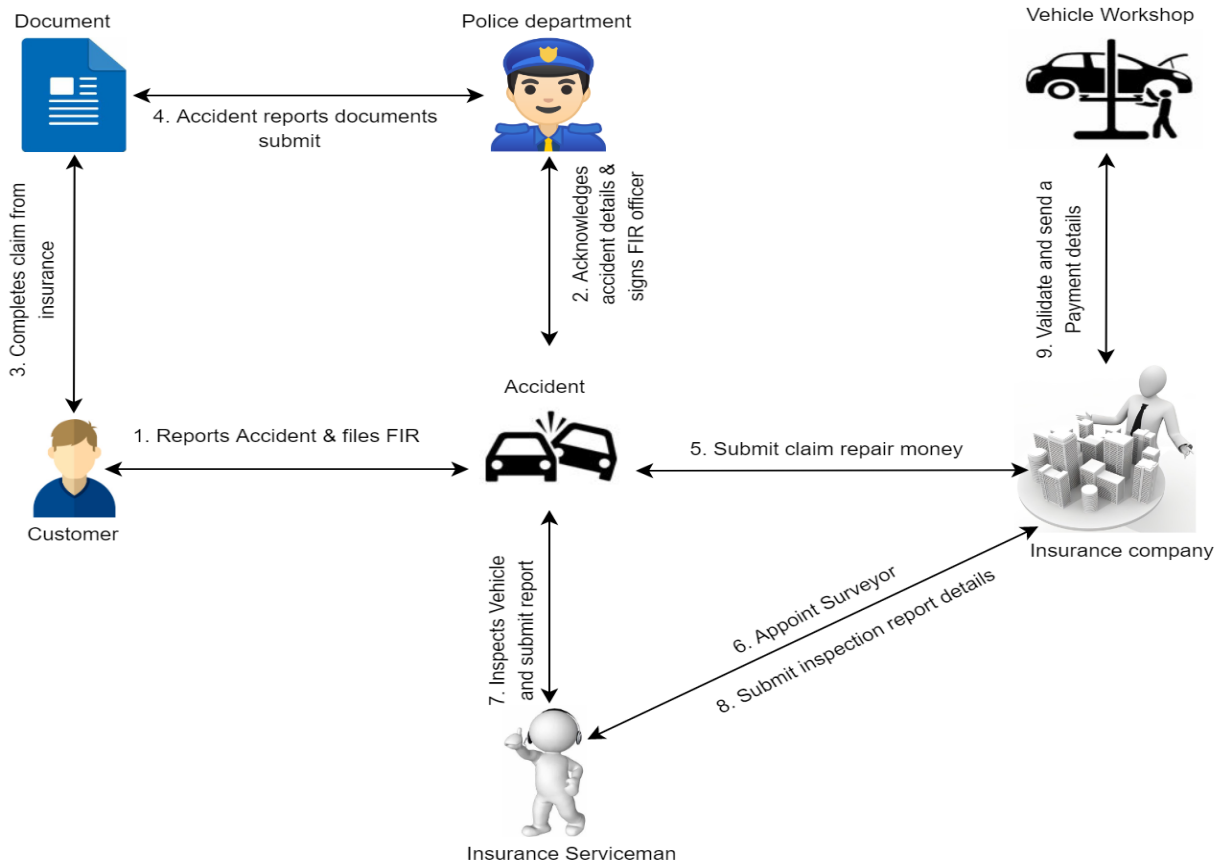


Figure 5. Proposed framework for Vehicle Insurance.

Presenting proof of insurance involves a significant amount of physical labour. Manual processes and identifiable physical systems are subject to fraud, such as creating fraudulent automobile insurance tickets and their subsequent sale (Dorri *et al.*, 2017). People are compelled to take such risks due to the high cost of insurance. There are many different contexts in which fraudulent acts relating to insurance documents can be committed. Due to the fact that the vast majority of drivers are requested to provide proof of insurance but are not contacted for official reasons, drivers can use cons to get out of tight and annoying situations. Various factors can lead to the misuse of the manual process as a means of communication between parties who lack mutual trust. These individuals and organisations rely on the accuracy and consistency of this information. Figure 4 depicts the vehicle insurance process without blockchain technology.

3.2 Proposed Framework for Vehicle Insurance-based Blockchain Framework

In this section, we discuss the proposed approach for a blockchain-based solution to the problem of regulating the functioning of the automotive insurance sector, as well as the management of claims, regulation of payments, and claim approvals. The blockchain-based solution proposed to strengthen the current vehicle insurance business and automatically route vehicle insurance claims is presented in Figure 6. It depicts the systems' constituent characters and entities. These parties consist of the policyholder (the customer), the vehicle insurance company, the representative from the garage, and the police department. The primary issue with the current framework is a lack of coordination among the many authorities (customer, insurance company, police department, vehicle workshop) (Guo & Yu, 2022). Other issues include ineffective administration of outdated cadastral records, insufficient utilization of information technology systems, significant opportunities for fraud and corruption, and so on. Blockchain, a game-changing technology capable of overcoming automobile insurance-related concerns, is one example of a new technology that has the potential to assist in addressing some of these critical issues.

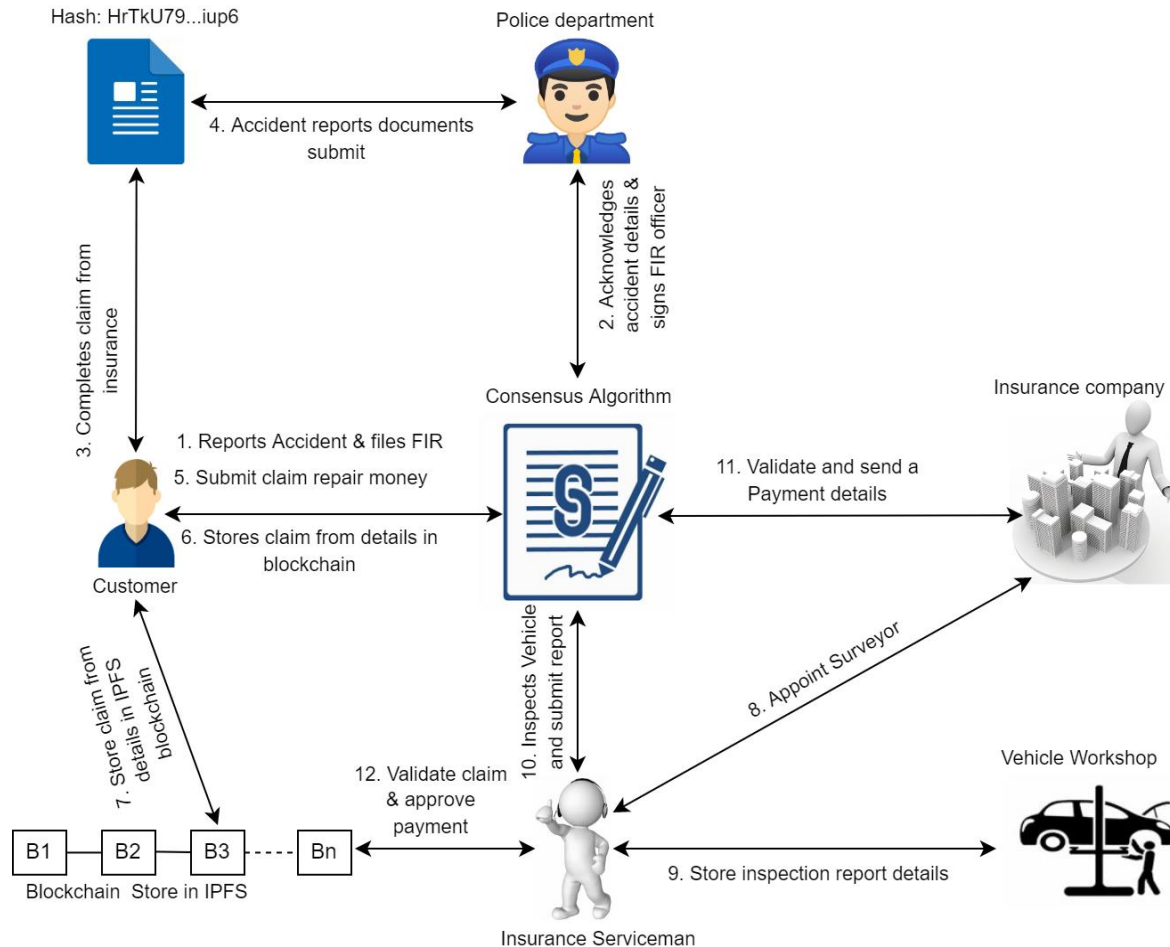


Figure 6. Vehicle Insurance-based Blockchain Framework Scenario.

The existing method of storing vehicle accident registries is inefficient and insecure. In the digital realm, hackers are prevalent and frequently attempt to violate information or steal data from their sources. The impossibility of breaking into blockchain-stored data is due to its powerful security measures. As everything is displayed on the network, the likelihood of discrepancies is very low. The majority of traditional models available on the market are expensive. By transferring all vehicle accident-related records to an immutable ledger, blockchain enables the secure storage of First Information Report (FIR) reports, insurance policies, and vehicle repair reports and eliminates common fraud sources in the insurance industry police bureau.

An SC executes a shared ledger and insurance policies to improve information storage. A blockchain is mainly used to prevent fraud and help recognise harmful behaviour patterns; it could begin with the sharing of fraudulent claims. Also, establishing ownership through digital certificates and reducing replication would eliminate double-booking and the processing of multiple claims for the same accident, as illustrated in Figure 5.

A blockchain that can create, exchange, and examine insurance records will provide stakeholders with a dependable platform for sharing information and a log of events (Demir *et al.*, 2019). Such an architecture can even record this shared event, and it makes sense to keep track of who requested it and with whom. The blockchain solution suggests unrestricted participation and democratic collective action. Every key player has the same rights, responsibilities, and costs. A higher standard of customer service, along with increased system automation levels, would benefit individuals. All parties stand to benefit from higher quality evidence in the event of a dispute.

Additionally, Blockchain improves both availability and dependability. With distributed administration, it would be impossible for one party to unilaterally change the data stored in ledgers, which is especially important when multiple parties have competing interests. Blockchain networks are more resistant to attacks that disrupt service or deny users access to the network. The solution to the problem of tracking insurance documents is a blockchain-based proposal that allows all participants to communicate, distribute, and record information.

The auto industry stands to benefit greatly from the use of blockchain, particularly in terms of eliminating middlemen and ensuring complete transparency and decentralisation. This will lead to lower costs for services and products, enhanced transaction processing security and anonymity of personal information, greater supply chain transparency, improved vehicle safety and data security, and more efficient fleet management, among other things. Additionally, using blockchain for transactions will allow businesses to audit records without the need for expensive and difficult-to-interpret systems. Some of the key benefits of using blockchain in the future of the auto industry include:

- **Increased efficiency:** Providing an overview of the entire value chain, automatic synchronisation of data, and more effective handling of contracts and collaborations.
- **Development of new products:** Offering Internet of Things (IoT), on-demand, pay-as-you-drive, and parametric insurance, as well as insurance between individuals.
- **Greater transparency:** Addressing customers' concerns about losing control of their data, enhancing the speed and security of data processing and sharing, and allowing customers to own their data and choose who can access it.
- **Automated processes:** Processing and verifying claims quickly and efficiently, making automatic payments, mapping multiple processes in a system to enhance efficiency (for

example, payments, contract signing, supply chain, document sharing, and protection against forgery), automating accounting transactions, and accelerating the payment of customers' claims.

3.3 Proposed Vehicle Insurance-based Blockchain Framework

Participants in the proposed blockchain network include individual drivers/owners, regional legal authorities, insurance companies, service technicians, auto manufacturing companies, and government regional transport offices, as illustrated in Figure 7. This technique will be converted into a blockchain-based application using the proposed framework. The multiple departmental registration offices are the network entities that will be involved in the proposed framework. These offices have each installed the validator on their respective machines. Together, these validator nodes and all other validator nodes dispersed worldwide will collaborate to build a shared P2P network.

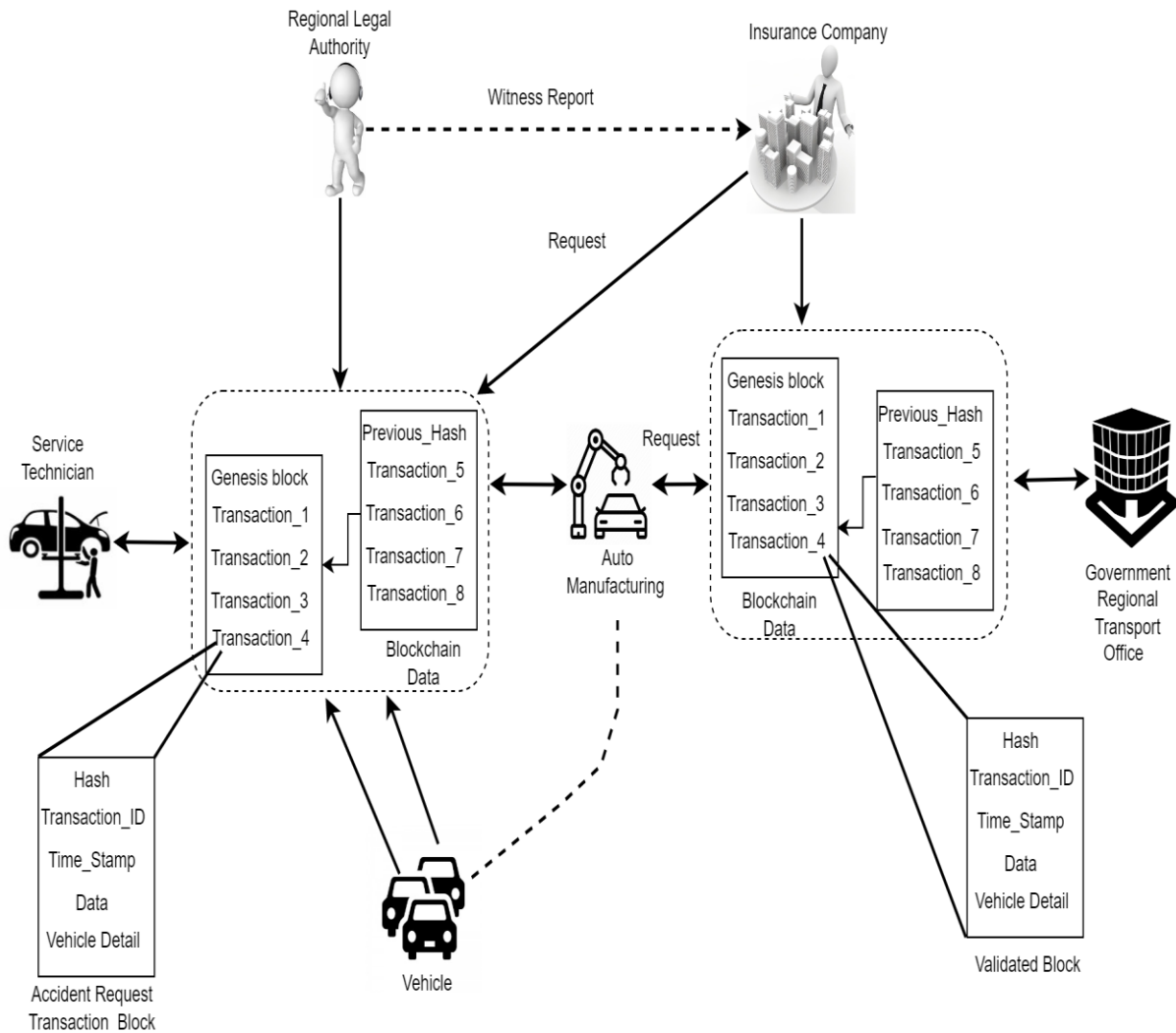


Figure 7. Proposed Vehicle Insurance-based Blockchain Framework.

The operational and decision segmentation form the division in our proposed paradigm. These partitions are designed to make it easier for users across our blockchain network to communicate pertinent information. When there is a disagreement, more convincing evidence benefits everyone. DLT also makes things more reliable and accessible. Distributed management would ensure that no party independently modifies the data, particularly if the parties have different goals.

We use the existing Public Key Infrastructure (PKI), like a Certificate Authority (CA), to give each blockchain participant, whether in the operational partition or the decision partition, a unique digital identity. This lets people talk through the blockchain. The certificate or verification part of the CA is kept in the genesis block, which is the first block in a blockchain and where it all starts. This component is used to authenticate and validate transactions.

In addition to the insurance provider being liable for compensation, all potentially responsible entities, such as linked and automated vehicles, auto manufacturers, and service technicians, are included in the operational partition. Although this work focusses on a single entity for each of these for simplicity, the framework is designed to apply to situations where there are several instances of each entity. It is assumed that the respective automakers meet the software update requirements of connected and automated vehicles. It is also assumed that a connected and automated vehicle connecting to 5G has tamper-proof storage for accident-related data like the exact location, speed, and time of the event, as well as video and picture data of the accident and data sent from witnesses via vehicular communication.

In the operational partition, the auto manufacturer, the service technician, and the connected and automated vehicles make up the group of proposers. In contrast, the insurance company, the service technician, and the auto manufacturer make up the validators. Validators are picked based on whether or not they possess sufficient capacity for processing blocks and transactions. Since validators could also send transactions in the blockchain data block, we use a “dual signature transactions” system to ensure that the recipient confirms the transaction started by a validator before it is added to the blockchain. This is done because validators may also send transactions within the blockchain data block. Because of this, a validator cannot create fictitious transactions to avoid responsibility.

Transactions in the blockchain data block can be signed either by a single participant, in which case these are referred to as single-sign transactions, or by numerous participants, in which case they are referred to as multiSig transactions. Participants can report safety events, offer primary evidence, issue specific instructions, or inform the execution of instructions through the key transactions contained within the blockchain data block. When a transaction is first added to a blockchain data block, verifying and validating it begins with a validator ensuring that the transaction producer is an allowed participant in the blockchain data block. This is the first thing you must do to check if something is true. After that, it checks to see if the transaction is complete. For example, a multiSig transaction is complete when all parties have signed it, and it is not a copy of another transaction that one of the parties has already sent. In the blockchain’s data block, it is assumed that validators will utilise previously defined keys to build a dynamic block. Following the completion of a successfully verified transaction, the transaction will be validated in the dynamic block by computing a new dynamic block.

4. Implementation of the Proposed Algorithm

In this section, we supply some of the crucial code snippets and algorithms related to the implementation of the proposed work. On a blockchain platform, the insurance transaction method,

accident transaction procedure, and repair transaction procedure claim functioning concept are each explained in detail by Algorithm 1, 2, and 3 respectively.

The Hyperledger platform allows developers to communicate data that may be addressed to specific content and facilitates mining policies and consensus methods. Each validator node that makes up the Hyperledger network has its specific address. A bootstrap server is used to establish a connection between a Hyperledger node and several other peers (other nodes) on the network. Regardless of where they are physically located, all validation nodes are connected and maintain the shared blockchain through the P2P swarm network. After the development of the proposed network model, the procedure of car insurance registration needs to be converted into a digital format. The following fundamental actions are often required to complete the process of registering a vehicle for insurance:

1. Insurance transaction procedure
2. Accident transaction procedure
3. Repair transaction procedure

The framework of the suggested architecture is designed to preserve the integrity of the policies while securely digitising and automating just the processes. The subsequent subsection explains the entirety of the transaction procedure.

4.1 Insurance transaction procedure through the proposed approach

In the proposed algorithm 1, only the insurer can verify the validity of the insurance. The insurer will look into the accident. If the accident was caused due to the irresponsibility of the driver, the insurer might decide to revoke the driver's insurance on that vehicle. Accordingly, the state of insurance will be changed to either 'valid' or 'invalid'. Then, all the information regarding the insurance, *i.e.*, the value of insurance, driver information, vehicle information, and information about the insurer, will be stored in the ledger, as illustrated in Figure 8. This algorithm enforces the rules for the validity of the smart insurance contract.

Blockchain is a technology that uses hash functions to ensure the validity of each block in a chain. Changes made to one block affect the entire chain, making it difficult to alter the ledger without being noticed. Blockchain replaces centralised control with a consensus mechanism, ensuring that no individual or group has control over the data stored on the blockchain. This decentralised trust is well-suited for handling insurance claims and reduces the likelihood of a single point of failure. The proposed architecture for a blockchain-based vehicle insurance framework provides automatic verification of insurance claims. This study uses blockchain and smart contracts to create a conceptual framework for insurance applications, with the main goal of ensuring safe transactions and preventing insurance fraud. The framework includes blockchain-based customer registration, policy issuance, and refund settlement, making the entire insurance system stronger. Blockchain entries are verified through a consensus mechanism.

Algorithm 1: Check Validity of Insurance Transaction Procedure

Input Variables

insurance: The insurance of the driver who had an accident

insurer: The insurer of the insurance

validity: Whether the insurance is valid or not

End Input Variables

-
1. **Procedure** CheckValidityInsurance (insurance, insurer, validity)
 2. get (insurance)
 3. insurance: validityrecord (insurance; insurer, vehicle, driver)
 4. insuranceContract.setInsurance(insurance)
 5. insuranceContract.setInsurer(insurer)
 6. insuranceContract.setVehicle(insurance.vehicle)
 7. insuranceContract.setDriver(insurance.driver)
 8. **End procedure**
-

```

Vehicle:
    vehicleId: EU002P230
    vehicleStatus: 'DAMAGED'

Driver:
    driverId: PY09056
    name: Alessa
    address: colony sector 214, Nh road, Paris
    balance: 500000

Insurer:
    Company: SBI
    Branch: pnb road, saf colony, Hjk

Insurance:
    insuranceId: 036878
    validity: VALID
    insurance value: Rs 1000000
    owner: Alessa
    vehicleId : EU002P230

```

Figure 8. A Sample Insurance.

4.2 Accident transaction procedure through the proposed approach

The proposed algorithm 2 makes it possible for any person to report an accident. The driver can also report the accident, but in the event of the driver's death, then any other person who witnessed the accident could feed the information in the report. After the accident, the vehicle's state will be changed from 'active' to 'damaged'. Also, the driver who was in the accident, the police to whom the accident was reported, the vehicle involved in the accident, information about witnesses, and the accident's location will be stored in the ledger illustrated in Figure 9 that describes the rules for reporting accident SCs.

Algorithm 2: Report Accident Transaction Procedure

Input Variables

driver: The driver who was in the accident
vehicle: The vehicle that was in the accident
police: The police who reported the accident
witness: The person who reported the accident to police

location: The location of the accident

End Input Variables

1. **Procedure** ReportAccident (driver, vehicleID, police, witness, location)
2. vehicle ← get(vehicleID)
3. vehicle.status ← DAMAGED
4. reportAccidentContract ← CreateReportAccidentContract()
5. reportAccidentContract.setDriver (driver)
6. reportAccidentContract.setVehicle(vehicle)
7. reportAccidentContract.setPolice(police)
8. reportAccidentContract.setWitness(witness)
9. reportAccidentContract.setLocation(location)

10. End procedure

Police:
Name: Mitch
Branch location: Paris
Vehicle:
vehicleId: EU002P230
vehicleStatus: 'DAMAGED'
Driver:
driverId: PY09056
name: Alessa
address: colony sector 214, Nh road, Paris
Location: cy street, bond road, Paris
Witness:
Name: Sabrina
address: nr. Haugh hotel, musieb road, Paris

Figure 9. A Sample Accident Report.

4.3 Repair transaction procedure through the proposed approach

The proposed algorithm 3 describes how the vehicle owner is responsible for repairing their vehicle. The vehicle is taken to a vehicle garage. The cost of repairs will either be covered by insurance or the driver's balance. If the insurance coverage exceeds the cost of repairs, the difference will be deducted from the owner's account. The rules for vehicle repair SCs will be stored in the ledger depicted in Figure 10, which will contain all information pertaining to the repair of the vehicle, including details about the owner, vehicle, insurance, garage, and cost of repairs.

Algorithm 3: Vehicle repair transaction procedure

Input Variables

driver: the driver who is repairing their vehicle

vehicle: the damaged vehicle that needs to be repaired

insurance: the insurance of the driver who had an accident

insurer: the insurer of the insurance

repairShop: the shop where the vehicle is repaired

costOfRepair: the cost of repair of the vehicle

end Input Variables

1: **Procedure**VehicleRepair(vehicle; driver; insurance; insurer; costOfRepair; repairShop)

2: get(insurance)

3: get(driver)

4: if insurance.checkvalid == 'VALID' **then**

5: if insurance.value \leftarrow costRepair **then**

6: driver.balance(costRepair \leftarrow insurance.value)

7: end if

8: end if

9: update(driver)

10: get(vehicle)

11: vehicle:vehicleStatus' \leftarrow ACTIVE'

12: update(vehicle)

13: VehicleRepairContract.setVehicle(vehicle)

14: VehicleRepairContract.setDriver(driver)

15: VehicleRepairContract.setInsurance(insurance)

16: VehicleRepairContract.setInsurer(insurer)

17: VehicleRepairContract.setCostOfRepair(costOfRepair)

18: VehicleRepairContract.setRepairShop(repairShop)

19: **End procedure**

Vehicle:	vehicleId: EU002P230
	vehicleStatus: 'DAMAGED'
Driver:	driverId: PY09056
	name: Alessa
	address: colony sector 214, Nh road, Paris
	balance: 400000
Insurer:	Company: SBI
	Branch: pnb road, saf colony, Hjk
Insurance:	insuranceld: 036878
	validity: VALID
	insurance value: Rs 1000000
	owner: Alessa
	vehicleid : EU002P230
Cost Of Repair:	1100000
Repair Shop:	Name: Lola Mechanics
	Address: colony sector 218, Nhk road, Paris

Figure 10. A sample vehicle repair contract.

4.4 Working of the Proposed Framework

In this architecture, blockchain technology is utilised to process and maintain a component of the insurance environment. Blockchain technology increases the accountability of the insurance industry while reducing the risk of fraudulent claims. Figure 11 depicts the fundamental use case functions of the framework. Using distributed SCs preserves these insurance policy features. These contracts are secure, trustworthy, and practically impossible to manipulate. The information regarding the customer and the policy will be stored in a database as an object using SCs. A closer examination reveals that the customer can sign up for the service and submit an application for the initialisation of the policy, as well as a claim and a refund. The agents and validators of the insurance company are part of the organisation's internal workforce. Validators have access to the mechanisms for claiming a policy, validating refunds, and validating transaction blocks.

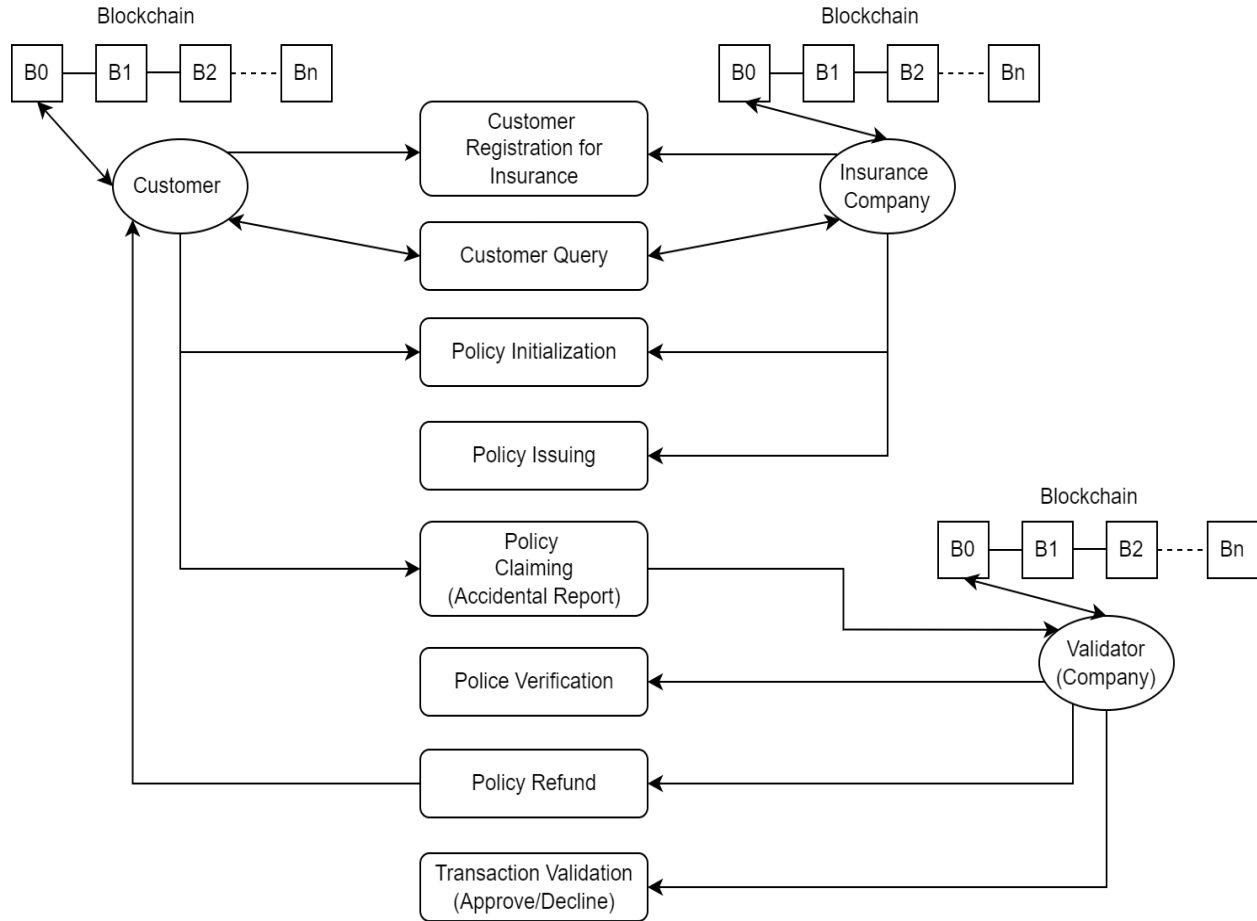


Figure 11. Flowchart of the Proposed Framework.

According to the rules stated for the insurance SC, when a customer submits a claim for a refund, the SC must inform the validator about the customer's account information. The validators examine the contract's specifics before communicating their decision to the parties involved. The operation of the process within the blockchain is governed by the set of rules outlined below:

1. Client registration

1. $StructOC \leftarrow (id, name, age, contact, history);$
2. $Database \leftarrow StructOC;$
3. $C_{key} \leftarrow f(Agent_id, Client_id);$
4. $Store (C_{key}, Object_{Client})$ in theBlockchain;

2. Client query

1. $C_{key} \leftarrow f(Agent_id, Client_id);$
2. Search (C_{key}) in the blockchain;
3. If(exists) retrieve desired $Object_{Client}$ Else return Error;

3. Policy initialisation

- (1) StructOP \leftarrow (Policy_id, Policy_name, Policy_Premium, Policy_Reimburse, Policy_Term);
- (2) StructOPC \leftarrow (Policy_id, Client_id, Amount, Acceptance, Date);
- (3) Store the structures in the Database;

4. Policy issuing

1. Check if the Object_{PolicyClient} already exists;
2. Check Client Smart Contract if Client with an id is registered to an Agent;
3. Check if Client Premium matches Policy Premium;
4. CkeyPolicyClient \leftarrow f (Agent_id, Client_id, Policy_id);
5. Object_{PolicyClient} \leftarrow new StructOPC(Client_id, Policy_id, 0, yes, date);
6. Store (CkeyPolicyClient, Object_{PolicyClient}) in the Blockchain;

5. Policy claiming

1. CkeyPolicyClient \leftarrow f (Agent_id, Client_id, Policy_id)
2. Check if the Object_{PolicyClient} exists using the CkeyPolicyClient
3. If Object_{PolicyClient} exists, check acceptance in Object_{PolicyClient};
- 4 if (acc==Yes) then
 if amt + Client_Reimburse \leq Policy_Reimburse then
 Refund(Agent_id, Client_id, Policy_id, Client_Reimburse)
 else
 Refund(Agent_id, Client_id, Policy_id, Policy_Reimburse-amt)
5. end;

5. Experimental Results and Analysis

The VARB runs successfully on a single host. In our proposed approach, any person near the accident can report the accident. The vehicle owner will then claim the vehicle's insurance, and the insurer will determine the validity of the insurance. Our blockchain network verifies that the insurance is only claimed for insured vehicles. The vehicle's insurance is also claimed only once for a particular accident, thus removing insurance fraud. The vehicle owner then repairs their vehicle, and the transaction is recorded in the ledger discussed in Table 1.

S. No.	Working Functions
1	Creation of a new vehicle for every owner when they purchase it.
2	The vehicle owner can apply for vehicle insurance.
3	The insurer can provide insurance to the vehicle owner.
4	Any third person can report an accident to the police.
5	The insurance adjuster can adjust the insurance holder's amount based on the damage caused to the vehicle.
6	Verify the true identity of the insurance holder.
7	Securely transfer the insurance amount to the owner.
8	The owner may repair the vehicle using either insurance funds or his own funds.

Validity is used to evaluate the performance of the proposed framework. The proposed VARN has been implemented on a Windows 10 machine running Hyperledger Fabric. Using a variety of computer hardware and software technologies, we have successfully established a decentralised structure, as evidenced by the default experimental parameter shown in Table 2.

Table 2. Hardware and software specifications	
Hardware	<ul style="list-style-type: none"> • CPU: Intel® Core™ i7-7700 CPU @ 3.60GHz 3.60 GHz • RAM: 16.00 GB
Software version	<ul style="list-style-type: none"> • Operating system: Windows • Hyperledger Fabric • Golang language • GCC compiler 10.2
Number of Nodes	<ul style="list-style-type: none"> • 4,8,16,32,64,128, 256
Transaction sending rate (s)	<ul style="list-style-type: none"> • 50,100,200,300, 400,500,600, 700, 800
Block size (KB)	<ul style="list-style-type: none"> • 8,16,32,64,128, 256,512,1024
Timer time out (ms)	<ul style="list-style-type: none"> • 50,75,100,200, 500,2000, 4000, 5000
Application	<ul style="list-style-type: none"> • Vehicle Accident Registry Network (VARN)

The standard experimental parameters are provided for the readers' convenience in Table 2. On the same server, we generate new virtual nodes with the go routine command of the Golang programming language. In certain situations, it can use the hardware resources available on our test bed. Each node possesses an internal programme that sends transactions to itself at a predetermined rate. It is unnecessary to consider the time between the transaction's sending and receiving. The rate at which transactions are sent is set to 500 tx/s by default. Depending on whether or not they need to be carried out on a machine running the Hyperledger Fabric Platform, these types of transactions can be categorised as either SCs or fixed-byte-length transactions. The block size refers to the maximum amount of storage space that a single block is allowed to occupy. The block size affects the batch size of the block buffer pool. The default size of each block is 256 kilobytes. The length of the transaction data generated by the system at random is known as the payload size. The default amount of storage space utilised by the payload of a transaction is 2048 bytes. A timer is contained within the buffer pool of the node and is reset whenever a new block is presented. If the timeout runs out, the transactions currently stored in the buffer pool will be bundled into a block proposal message. If the total number of transactions in the buffer pool exceeds the amount of data contained in the block, the node will make an additional effort to propose a new block. In this section, we look at how the proposed architecture compares to Bitcoin's Proof of Work (PoW) regarding the number of messages that need to be sent before consensus is reached. Assuming the network has N nodes, in the PoW method, all N nodes reach a consensus, and each one sends its vote to all $N-1$ nodes. So, PoW requires a total of $N(N-1)$ messages sent back and forth. In the proposed architecture, only half of the cluster nodes participate in the consensus process. Let us assume that each cluster has m nodes and that there are t clusters in the network. Thus, the total number of nodes involved in sending and receiving messages is $t(m(50/100))$. The proposed architecture requires fewer messages than Bitcoin to reach a consensus.

5.1 Block Approval Time

The number of miners remains constant, but the number of blocks in the blockchain varies. Miners need to access the blockchain to gather information about vehicles and insurance, after which they send back the status of the validity of transactions. Figure 12 presents a comparison between the number of blocks and the time it takes to mine each block. Block approval time is recorded for blocks ranging from 0 to 40.

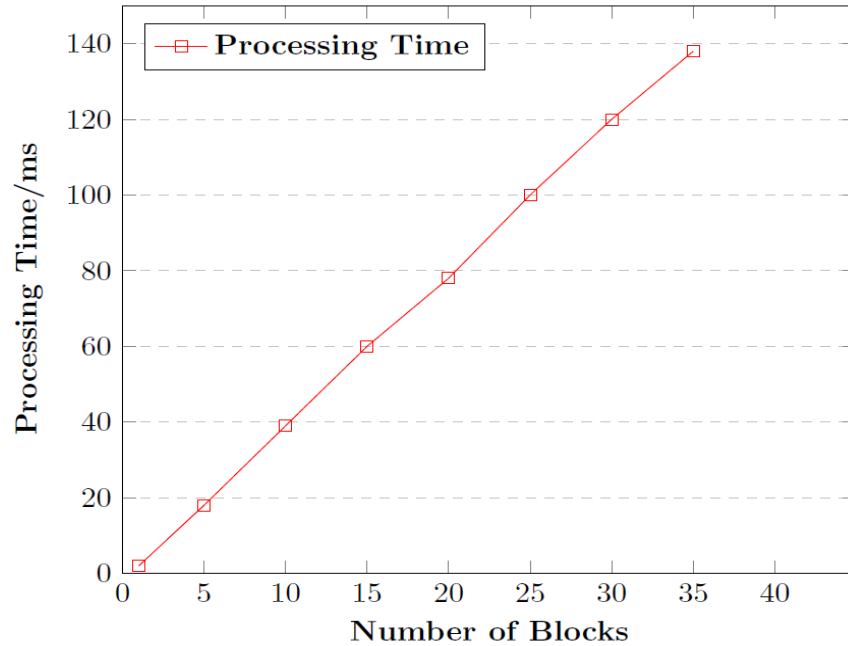


Figure 12. Number of Blocks vs. Processing Time to Mine Each Block.

Figure 13 illustrates the time it takes for transactions to be processed on the Bitcoin network. It shows that the proposed architecture takes less time than the Bitcoin network to copy data and update the ledger. A region-based architecture is used in our proposed structure. This means that all nodes can see all the information. As the number of blocks increases, Bitcoin network requires approximately 2.1 times more time than our suggested architecture to duplicate data. The discrepancy in processing times between the two approaches widens as the number of blocks in the network increases.

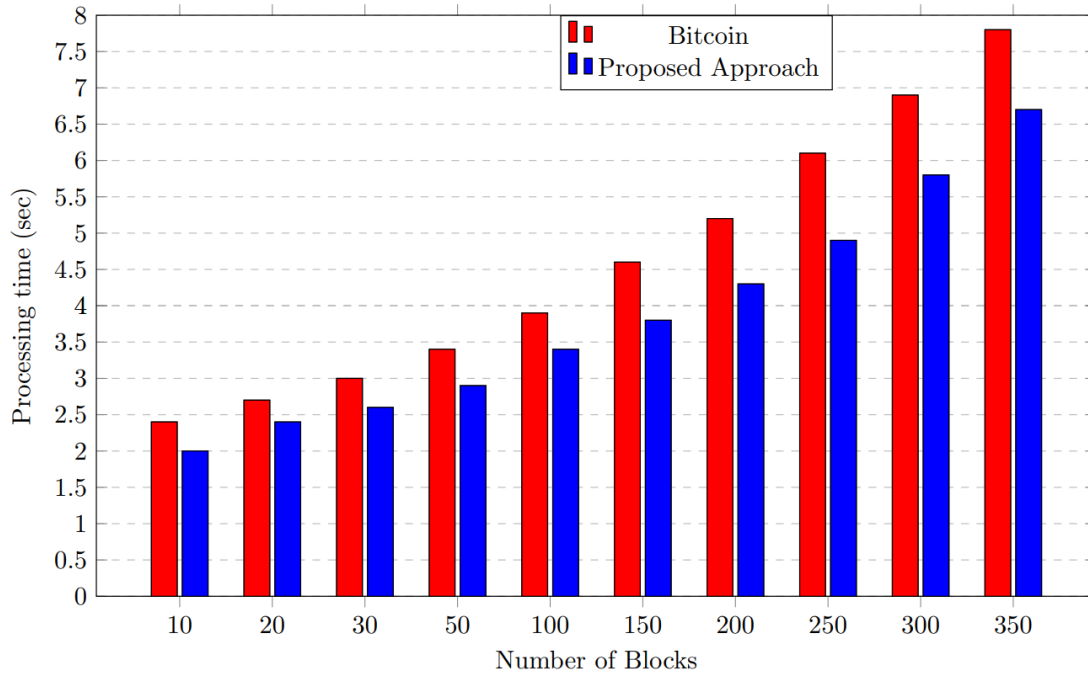


Figure 13. Processing Time for Bitcoin vs. Proposed Approach when the Number of Blocks Increases.

Figure 14 illustrates the processing time required to ensure consistency by bringing each Bitcoin network node up to date on the ledger, as well as the suggested design and the impact of adding more nodes. It demonstrates that our proposed architecture is capable of providing a faster response time than the Bitcoin network.

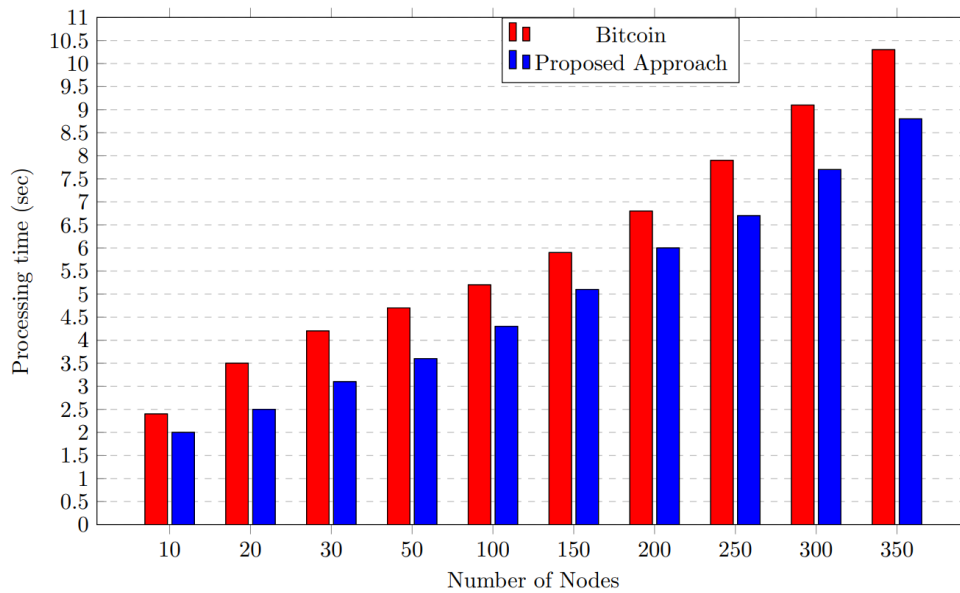


Figure 14. Processing Time for Bitcoin vs. Proposed Approach when the Number of Nodes Increases.

Our proposed architecture achieves faster data transfer in the network, as it is about 20 times faster when the number of network nodes increases. In addition, compared to the Bitcoin network, our architecture improves the processing time required for replicating data and updating the ledger by an average of over 73%.

6. Security and Privacy Analysis

Every insurance system is responsible for protecting its services' confidentiality, availability, and honesty. It is possible to maintain information confidentiality if it is not disclosed to users who are not authorised to receive it. It is possible to maintain information integrity if it is protected from any modification; and it is possible to maintain information availability if it can be accessed when it is required without being vulnerable to denial-of-service attacks, distributed denial of service attacks, or other similar types of service disruptions. This section presents a qualitative theoretical examination of the performance of the vehicle insurance-based blockchain framework privacy and security features.

Using public key cryptography, the records that are stored in the proposed system are protected against malicious attempts to alter them and unauthorized access. During this time, each network user is issued a private key that can be used to verify and sign the transactions. The network uses encryption and digital signatures to ensure the security and confidentiality of stored records and to control access to these files. Furthermore, to change a record in most blockchains, an attacker must control 51% of the network peers (using PoW, PoS, or DPoS as examples) (Dorri *et al.*, 2017). This is practically impossible to achieve. To alter any block in the blockchain, an attacker must first alter all instances of that block across the network and then persuade the majority of nodes that the altered block is the authoritative one.

In addition, the proposed network will hash all user blocks and store unreadable hashes of transactions. This will make it possible to maintain a higher level of privacy over the data that are stored in the network. The proposed system is a decentralised peer-to-peer network with multiple nodes storing user data. This helps to ensure the system's availability by removing any potential weak spots in the infrastructure. By registering a node before it can start exchanging data with the rest of the network peers, DPoS makes it harder for an adversary to launch denial-of-service (DoS) or Distributed DoS (DDoS) attacks against the system. All network node transactions are checked by the witnesses to make sure they are valid. This makes it harder to do.

The proposed architecture utilises blockchain as a distributed system to protect against DoS attacks. It is difficult for an attacker to flood all nodes at once, as this would stop the system from functioning. Even if some nodes are compromised, the system can still provide services as a whole.

In a DoS attack, a malicious user might send numerous invalid transactions to the network, making it difficult for legitimate users to use the system. However, since the proposed architecture is distributed and transaction allocation is based on the most significant bit, it is impossible for a user to send transactions to a specific blockchain. This feature makes the proposed blockchain-based architecture secure against DoS attacks.

Table 3 summarises the security services and measures part of the proposed framework. Transactions are kept private and safe with these services and steps. To get the most out of computers, user devices will run a lightweight client to store transactions instead of a full copy of the blockchain, which is more expensive (Hu & Chen, 2022). It is possible to get a high throughput using blockchain technology and consensus protocols like PoW, PoS, and DPoS, which keep scalability, speed, interoperability, and transparency (Bie *et al.*, 2022).

Security service	Countermeasure
Authentication	The address on the blockchain and the digital signature
Access control	Signing with a digital signature and encrypting the data
Confidentiality	Encryption
Integrity	Encryption technology and electronic signatures
Non-repudiation	Encryption and digital signatures are both available
Availability	Distributed/Decentralised
Trust	Encrypted, decentralised, and with a digital signature

The proposed framework implements encryption and digital signatures using the Elliptic Curve Cryptography (ECC) method, which is standard for most existing blockchain systems like Bitcoin and Ethereum. The vast majority of other blockchain technologies also use this method. ECC and RSA offer equivalent levels of protection. However, RSA requires a substantially greater number of bits than ECC. For instance, the amount of security offered by an ECC key with 256 bits is equivalent to that of an RSA key with 3072 bits (Deshmukh *et al.*, 2022).

In most cases, a shorter key will result in less processing power, less memory, and faster key production. These gains are also advantageous to the proposed framework, as they speed up the output of transactions and the closing of blocks, which are both essential steps in the process. The RSA and ECC key length studies are broken down and summarised in Table 4. Most applications use 256-bit ECC keys because they provide the necessary level of security. Blockchain technology makes extensive use of these keys.

RSA key length	ECC key length	Approx. ratio (RSA:ECC)
1024	160	7:1
2048	224	10:1
3072	256	13:1
7680	348	22:1
15360	512	30:1

Table 5 summarises the many advantages that can be gained from using an electronic government system based on blockchain technology. These advantages encompass crucial aspects such as security and privacy, which continue to be of utmost importance in today's data-driven world (Charles *et al.*, 2015). Due to these qualities, blockchain technology has become a possible candidate for use as a trend in implementing insurance systems. That has the potential to offer a communication channel between the public sector and the citizens that is easy to use, safe, and resistant to errors. Because of the indirect benefits of blockchain technologies, such as the reduction of bureaucracy, the elimination of paper use, the reduction of transaction costs, and the control of corruption, the government ecosystem may change in a way that makes it easier for people to trust the government (Deshmukh *et al.*, 2022).

Table 5. The characteristics of an insurance system based on blockchain technology (Guo & Yu, 2022)	
Feature	Justification
Reduced human errors	Before granting access to the network, user identities and devices are verified and authenticated.
Increased public trust	All network participants' identities are validated to ensure that users can trust the data they share.
Greater scalability	By the consensus mechanism, the system can scale up to accommodate additional users and devices readily, and this expansion can take place automatically.
Improved reliability	There are several servers and storage places where data can be found. The consensus process assures that changes to the data may only be made with the agreement of all participants in the study.
Increased resiliency	The system will be more resistant to viruses, DoS assaults, and DDoS attacks if it does not have any single points of failure.
Improved auditability	Due to the network's immutability, it is simple to reconstruct the history of all transactions.
Greater verifiability	Before being added to the blockchain, each new transaction is validated by every network participant.
Information ownership	Individuals are accountable for authorising access to their information.
Improved access to information	Multiple locations are used to store data, which facilitates easy and quick access.
Increased data quality	All records and transactions stored in the system are checked in advance to ensure they are legitimate.
Greater transparency	Based on this consensus mechanism, all nodes in the network agree on which further transactions should be added.
Reduced operational costs	A third-party entity need not process transactions because this is not required.
Improved efficiency and speed	The new records are distributed to all the nodes in the network, and anyone with access to the network can examine any record with the accessibility privilege.

7. Managerial Implications

The adoption of a blockchain-based secure privacy-preserving vehicle accident and insurance registration framework has several managerial implications for insurance companies.

First, the main aim of any insurance company is to maximise its business and profitability. By adopting a blockchain-based secure privacy-preserving vehicle accident and insurance registration framework, insurance companies can ensure faster and fairer settlement claims. This will not only increase the trust of policyholders but also result in greater customer satisfaction. This could also lead to increased customer loyalty and retention, as customers will be more likely to stick with an insurance company that provides a secure and transparent claims process. Additionally, with increased customer satisfaction, insurance companies can expect to see reduced churn rates and increased customer lifetime value.

Second, the proposed application would lead to widespread popularity of the insurance company adopting it, and hence its market share, too. Insurance companies that adopt such advanced technologies and practices tend to have a competitive edge over their rivals. This could also potentially attract new customers who value transparency and security. In addition to gaining new customers, implementing the proposed solution can also result in cost savings for insurance companies due to increased efficiency in claims processing and reduced fraud.

Third, the proposed application can be further enhanced by including financial interoperability solutions using e-wallets and blockchain, as proposed by the authors in Singh *et al.* (2018). This would enable policyholders to seamlessly make premium payments and receive claim settlements, further improving the overall customer experience.

In conclusion, the adoption of the proposed blockchain-based secure privacy-preserving vehicle accident and insurance registration framework has numerous benefits for insurance companies, including improved efficiency, customer satisfaction, and competitiveness. By staying at the forefront of technological advancements, insurance companies can create a sustainable competitive advantage and ensure long-term success.

8. Conclusion

In this research paper, blockchain technology is used to process and maintain a component of the insurance environment. Blockchain technology increases the accountability of the insurance industry while reducing the risk of fraudulent claims. The proposed work implements a novel use case consisting of a vehicle insurance-based blockchain framework solution built on a Hyperledger Fabric network for a vehicle insurance network. The proposed Vehicle Accident Register Blockchain (VARB), which is based on Hyperledger, takes a problem-centric thinking approach (Charles *et al.*, 2022) and makes use of various assets, participants, and transactions. Individual drivers/owners, regional legal authorities, insurance companies, service technicians, auto manufacturing companies, and government regional transport offices are participants in the proposed blockchain network. Using distributed smart contracts preserves these insurance policy features. These contracts are secure, trustworthy, and practically impossible to manipulate. The experimental results demonstrate that as the number of blocks increases, the Bitcoin network requires approximately 2.1 times longer than our suggested architecture to duplicate data. The discrepancy in processing times between the two approaches widens as the number of blocks in the network increases. When the number of network nodes increases, the network transfer of data is about 20 times faster. In addition, compared to the Bitcoin network, our architecture improves the processing time required for replicating data and updating the ledger by an average of over 73%. Indirect benefits of the proposed robust blockchain-based vehicle insurance framework include lowering transaction costs and preventing corruption. This could change the way governments work in a way that makes it easier for people to trust their governments.

Although this research provides valuable insights into the use of blockchain technology, there are several limitations that should be acknowledged. One of the primary limitations is the lack of a generic and uniform blockchain architecture. This means that further analysis is needed in this area to develop a more comprehensive understanding of blockchain architecture and its applications. Another limitation of the study is related to the increasing load on the blockchain scheme. As more transactions are processed, the blockchain becomes larger and storing it becomes more challenging. To address this challenge, efficient search algorithms are required to enable quick and efficient search operations on the blockchain. Therefore, future research should focus on developing and implementing efficient search algorithms that can support the scalability and

efficiency of blockchain technology. An additional limitation of this research is that it is primarily a conceptual paper and lacks empirical data to support the proposed framework. Therefore, further research is required to validate the effectiveness and feasibility of the proposed approach in a practical setting.

Finally, we identify future research directions that we will explore in our upcoming work. One of our aims is to extend the proposed model to address open issues. Specifically, we plan to extend this work to develop a VARB for reporting hospital, home, and police accidents insurance. As blockchain gains popularity, it is essential to improve algorithms based on platform- and product-specific requirements. Our proposed solution prioritises efficiency, scalability, transparency, and modularity, and can thus be implemented in any country. We further intend to provide formal security proof for the proposed model and investigate whether an insurance pool can utilise blockchain technology to invest the money it collects. This approach could encourage banks and insurance companies to join the proposed collaborative insurance system. Lastly, as this is a conceptual paper, further empirical testing is required to validate the proposed model.

Acknowledgments: The authors would like to thank the Editor-in-Chief, the Associate Editor, and the anonymous reviewers for their valuable feedback on the previous version of this manuscript.

References

- Bader, L., Burger, J. C., Matzutt, R., & Wehrle, K. (2018). Smart Contract-Based Car Insurance Policies. *2018 IEEE Globecom Workshops (GC Wkshps)*, 1–7. <https://doi.org/10.1109/GLOCOMW.2018.8644136>
- Benhamouda, F., Halevi, S., & Halevi, T. (2019). Supporting private data on Hyperledger Fabric with secure multiparty computation. *IBM Journal of Research and Development*, 63(2/3), 3:1-3:8. <https://doi.org/10.1147/JRD.2019.2913621>
- 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>
- Bie, M., Li, W., Chen, T., Nan, L., & Yang, D. (2022). An energy-efficient reconfigurable asymmetric modular cryptographic operation unit for RSA and ECC. *Frontiers of Information Technology & Electronic Engineering*, 23(1), 134–144. <https://doi.org/10.1631/FITEE.2000325>
- Charles, V., Emrouznejad, A., & Gherman, T. (2023). A critical analysis of the integration of blockchain and artificial intelligence for supply chain. *Annals of Operations Research*, 1-44. <https://doi.org/10.1007/s10479-023-05169-w>
- Charles, V., Emrouznejad, A., Gherman, T., & Cochran, J. (2022). Why Data Analytics is an Art. *Significance*, 19(6), 42–45. <https://doi.org/10.1111/1740-9713.01707>
- Charles, V., Tavana, M., & Gherman, T. (2015). The right to be forgotten – is privacy sold out in the big data age? *International Journal of Society Systems Science*, 7(4), 283–298. <https://doi.org/10.1504/IJSSS.2015.073225>
- Demir, M., Turetken, O., & Ferworn, A. (2019). Blockchain Based Transparent Vehicle Insurance Management. *2019 Sixth International Conference on Software Defined Systems (SDS)*, 213–220. <https://doi.org/10.1109/SDS.2019.8768669>

- Deshmukh, A., Sreenath, N., Tyagi, A. K., & Abhichandan, U. V. E. (2022). Blockchain Enabled Cyber Security: A Comprehensive Survey. *2022 International Conference on Computer Communication and Informatics (ICCCI)*, 1–6.
- Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020). A Secure AI-Driven Architecture for Automated Insurance Systems: Fraud Detection and Risk Measurement. *IEEE Access*, 8, 58546–58558. <https://doi.org/10.1109/ACCESS.2020.2983300>
- Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017). BlockChain: A Distributed Solution to Automotive Security and Privacy. *IEEE Communications Magazine*, 55(12), 119–125. <https://doi.org/10.1109/MCOM.2017.1700879>
- Emrouznejad, A., & Charles, V. (2022). *Big Data and Blockchain for Service Operations Management*. Cham: Springer.
- Gera, J., Palakayala, A. R., Rejeti, V. K. K., & Anusha, T. (2020). Blockchain Technology for Fraudulent Practices in Insurance Claim Process. *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, 1068–1075. <https://doi.org/10.1109/ICCES48766.2020.9138012>
- Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain: Research and Applications*, 3(2), 100067. <https://doi.org/10.1016/j.bcr.2022.100067>
- Gupta, S., Ghardallou, W., Pandey, D. K., & Sahu, G. P. (2022). Artificial intelligence adoption in the insurance industry: Evidence using the technology–organization–environment framework. *Research in International Business and Finance*, 63, 101757. <https://doi.org/10.1016/j.ribaf.2022.101757>
- Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*, 177, 102857. <https://doi.org/10.1016/j.jnca.2020.102857>
- Hu, W., & Chen, Y. (2022). Application of Artificial Intelligence in Financial Risk Management. In X. Sun, X. Zhang, Z. Xia, & E. Bertino (eds.), *Artificial Intelligence and Security. ICAIS 2022. Lecture Notes in Computer Science 13338* (pp. 180–188). Cham: Springer. https://doi.org/10.1007/978-3-031-06794-5_15
- Iyer, V., Shah, K., Rane, S., & Shankarmani, R. (2021). Decentralised Peer-to-Peer Crop Insurance. *Proceedings of the 3rd ACM International Symposium on Blockchain and Secure Critical Infrastructure*, 3–12. <https://doi.org/10.1145/3457337.3457837>
- Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Networking and Applications*, 14(5), 2901–2925. <https://doi.org/10.1007/s12083-021-01127-0>
- Kocsis, I., Pataricza, A., Telek, M., Klenik, A., Deé, F., & Cseh, D. (2017). *Towards performance modeling of hyperledger fabric*. International IBM Cloud Academy Conference (ICACON), Wroclaw, Poland.
- Kshetri, N. (2021). Blockchain-Based Smart Contracts to Provide Crop Insurance for Smallholder Farmers in Developing Countries. *IT Professional*, 23(6), 58–61. <https://doi.org/10.1109/MITP.2021.3123416>
- Manevich, Y., Barger, A., & Tock, Y. (2019). Endorsement in Hyperledger Fabric via service discovery. *IBM Journal of Research and Development*, 63(2/3), 2:1-2:9. <https://doi.org/10.1147/JRD.2019.2900647>
- Nakamoto, S. (2009). Bitcoin: a peer-to-peer electronic cash system. *Bitcoin White Paper*.
- Nanda, S. K., Panda, S. K., Das, M., & Satapathy, S. C. (2023). Decentralization of Car Insurance System Using Machine Learning and Distributed Ledger Technology. In V. Bhateja, X. S.

- Yang, J. Chun-Wei Lin, & R. Das (eds.), *Intelligent Data Engineering and Analytics. Proceedings of the 10th International Conference on Frontiers in Intelligent Computing: Theory and Applications (FICTA 2022)* (pp. 587–600). Singapore: Springer. https://doi.org/10.1007/978-981-19-7524-0_52
- Nizamuddin, N., & Abugabah, A. (2021). Blockchain for automotive: An insight towards the IPFS blockchain-based auto insurance sector. *International Journal of Electrical and Computer Engineering*, 11(3), 2443. <https://doi.org/10.11591/ijece.v11i3.pp2443-2456>
- Nunez Mencias, A., Dillenberger, D., Novotny, P., Toth, F., Morris, T. E., Paprotski, V., Dayka, J., Visegrady, T., OFarrell, B., Lang, J., & Carbarnes, E. (2018). An optimized blockchain solution for the IBM z14. *IBM Journal of Research and Development*, 62(2/3), 4:1-4:11. <https://doi.org/10.1147/JRD.2018.2795889>
- Oham, C., Jurdak, R., Kanhere, S. S., Dorri, A., & Jha, S. (2018). B-FICA: BlockChain based Framework for Auto-Insurance Claim and Adjudication. *2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1171–1180. https://doi.org/10.1109/Cybermatics_2018.2018.00210
- Parlak, M. (2023). Blockchain-based Immutable Evidence and Decentralized Loss Adjustment for Autonomous Vehicle Accidents in Insurance. *ArXiv Preprint ArXiv:2303.18130*.
- Pawar, V., & Sachdeva, S. (2023). ParallelChain: a scalable healthcare framework with low-energy consumption using blockchain. *International Transactions in Operational Research*, 1-29. <https://doi.org/10.1111/itor.13278>
- Pratticò, F. G., Lamberti, F., Cannavò, A., Morra, L., & Montuschi, P. (2021). Comparing state-of-the-art and emerging augmented reality interfaces for autonomous vehicle-to-pedestrian communication. *IEEE Transactions on Vehicular Technology*, 70(2), 1157–1168.
- Raikwar, M., Mazumdar, S., Ruj, S., Sen Gupta, S., Chattopadhyay, A., & Lam, K.-Y. (2018). A Blockchain Framework for Insurance Processes. *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 1–4. <https://doi.org/10.1109/NTMS.2018.8328731>
- Reebadiya, D., Rathod, T., Gupta, R., Tanwar, S., & Kumar, N. (2021). Blockchain-based Secure and Intelligent Sensing Scheme for Autonomous Vehicles Activity Tracking Beyond 5G Networks. *Peer-to-Peer Networking and Applications*, 14(5), 2757–2774. <https://doi.org/10.1007/s12083-021-01073-x>
- Salem, M. J., Ndolu, F. H. E., Hidayatullah, D. E. R., & Sari, R. F. (2021). Developing NEO Smart Contract for Weather-Based Insurance. *2021 4th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 603–608. <https://doi.org/10.1109/ISRITI54043.2021.9702853>
- Shetty, A., Shetty, A. D., Pai, R. Y., Rao, R. R., Bhandary, R., Shetty, J., Nayak, S., Keerthi Dinesh, T., & Dsouza, K. J. (2022). Block Chain Application in Insurance Services: A Systematic Review of the Evidence. *SAGE Open*, 12(1), 215824402210798. <https://doi.org/10.1177/21582440221079877>
- Singh, K., Singh, N., & Singh Kushwaha, D. (2018). An Interoperable and Secure E-Wallet Architecture based on Digital Ledger Technology using Blockchain. *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, 165–169. <https://doi.org/10.1109/GUCON.2018.8674919>
- Singh, M., & Kim, S. (2018). Branch based blockchain technology in intelligent vehicle. *Computer Networks*, 145, 219–231. <https://doi.org/10.1016/J.COMNET.2018.08.016>

- Statista. (2022). *Forecast of the global insurance market in 2021 and 2022, with forecasts from 2023 to 2026 (in billion U.S. dollars)*. Available at <https://www.statista.com/statistics/1192960/forecast-global-insurance-market/>
- Syed, T. A., Siddique, M. S., Nadeem, A., Alzahrani, A., Jan, S., & Khattak, M. A. K. (2020). A Novel Blockchain-Based Framework for Vehicle Life Cycle Tracking: An End-to-End Solution. *IEEE Access*, 8, 111042–111063. <https://doi.org/10.1109/ACCESS.2020.3002170>
- Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F.-Y. (2019). Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(11), 2266–2277. <https://doi.org/10.1109/TSMC.2019.2895123>
- Xiong, H., Dalhaus, T., Wang, P., & Huang, J. (2020). Blockchain Technology for Agriculture: Applications and Rationale. *Frontiers in Blockchain*, 3. <https://doi.org/10.3389/fbloc.2020.00007>
- Yadav, A. S., Singh, N., & Kushwaha, D. S. (2022a). A scalable trust based consensus mechanism for secure and tamper free property transaction mechanism using DLT. *International Journal of System Assurance Engineering and Management*, 13(2), 735–751. <https://doi.org/10.1007/s13198-021-01335-0>
- Yadav, A. S., Singh, N., & Kushwaha, D. S. (2022b). Sidechain: storage land registry data using blockchain improve performance of search records. *Cluster Computing*, 25(2), 1475–1495. <https://doi.org/10.1007/s10586-022-03535-0>
- Yadav, A. S., Singh, N., & Kushwaha, D. S. (2023). Evolution of Blockchain and consensus mechanisms & its real-world applications. *Multimedia Tools and Applications*, 1-46. <https://doi.org/10.1007/s11042-023-14624-6>

----- Forwarded message -----

From: **Binshan Lin** <em@editorialmanager.com>
Date: Tue, 30 May 2023 at 20:59
Subject: Your Submission ESWA-D-23-00721R2
To: Dharen Kumar Pandey <dharenp@gmail.com>

Ms. Ref. No.: ESWA-D-23-00721R2
Title: Blockchain-based Secure Privacy-Preserving Vehicle Accident and Insurance
Registration
Expert Systems With Applications

Dear Dr. Dharen Kumar Pandey,

As Editor-in-Chief, I'm pleased to inform you that I have accepted the above paper for publication in Expert Systems with Applications (ESWA). Your accepted manuscript will now be transferred to our production department and work will begin on creation of the proof. If we need any additional information to create the proof, we will let you know. If not, you will be contacted again in the next few days with a request to approve the proof and to complete a number of online forms that are required for publication. Your paper should appear as an "article in proofs" within two weeks of acceptance on ScienceDirect, and your printed version should appear in the journal within 2-3 months.

Please note that the authors' affiliations must be the institutions where the research presented in the article took place.

- ESWA has 2021 Impact Factor of 8.665, based on the Journal Citation Reports by Clarivate Analytics (released in June 2022).
- ESWA has 2021 CiteScore of 12.20 (released in June 2022).

We look forward to your continued participation in our journal, and we hope you will consider us again for future submissions.

With kind regards,

Dr. Binshan Lin
BellSouth Professor
Editor-in-Chief, Expert Systems with Applications
Editor-in-Chief, Machine Learning with Applications
Louisiana State University Shreveport
Email: Binshan.Lin@LSUS.edu