IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 7 April 2024, accepted 27 April 2024, date of publication 6 May 2024, date of current version 13 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3397059

RESEARCH ARTICLE

A Framework for Platform-Agnostic Blockchain and IoT Based Insurance System

J. GURUPRAKASH[1], DIMITAR TOKMAKOV[2], L. B. KRITHIKA[3], SRINIVAS KOPPU[3], R. SRINIVASA PERUMAL[4], ANNA BEKYAROVA-TOKMAKOVA[2], AND MIHAIL MILEV[2]

[1]Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Coimbatore 601103, India
[2]Faculty of Physics and Technology, University of Plovdiv Paisii Hilendarski, 4000 Plovdiv, Bulgaria
[3]School of Computer Science Engineering and Information Systems, Vellore Institute of Technology, Vellore 632014, India
[4]School of Computer Science and Engineering, Vellore Institute of Technology, Chennai 600127, India

Corresponding author: Dimitar Tokmakov (tokmakov@uni-plovdiv.bg)

This work was supported by the European Union-NextGenerationEU, through the National Recovery and Resilience Plan of the Republic of Bulgaria, under Project BG-RRP-2.004-0001-C01.

ABSTRACT Blockchain technology has the potential to revolutionize the insurance industry by bringing unprecedented levels of transparency, security and autonomous continuity. By leveraging this technology, insurance companies can streamline their processes, reduce costs and provide better services to their customers. The proposed framework represents a significant step forward in the industry's evolution, with the potential to create a more efficient and effective insurance ecosystem for all stakeholders involved. This framework offers a new and innovative approach to address many of the challenges associated with traditional processes in the insurance applications. By utilizing Blockchain and Internet of Things (IoT) technologies, the framework aims to provide greater transparency, security, efficiency and real-time data decision ultimately leading to an improved customer experience. The accomplished work serves as a foundation for further research and development in the field of blockchain-based insurance applications, with the goal of designing a lightweight, platform-agnostic, auditable, real-time and provable solution.

INDEX TERMS Blockchain, insurance.

I. INTRODUCTION

Blockchain technology, at its core, is a distributed ledger that stores and shares data among peers. This decentralized system groups data into "blocks," which must be verified by consensus within the ecosystem before becoming valid and authentic. Fig. 1 presents a conventional blockchain, special nodes called "miners" validate the transactions and aggregate them to blocks, with incentives provided through native cryptocurrency or other mechanisms. Once validated, blocks are permanently added to the chain. Blockchain users possess unique public and private keys that, when combined, serve to authenticate their identity [1].

Insurance plays a vital role in providing financial protection against various risks and uncertainties. The insurance industry has been undergoing a digital transformation, embracing new technologies to improve efficiency, transparency and customer experience. One such technology that has the potential to revolutionize the insurance sector is blockchain [1].

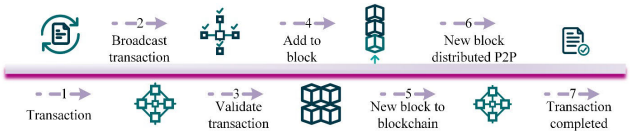


FIGURE 1. Generic flow of transactions in a blockchain.

Despite the advancements and market prediction on insurance industry as in Fig. 2, several challenges persist. These include lack of transparency, inefficient claim processing, fraud and limited customer engagement [2]. Traditional insurance systems often rely on manual processes and intermediaries, leading to higher costs and delays in claim settlements. Moreover, the centralized nature of these systems makes them vulnerable to data breaches and manipulation.

The associate editor coordinating the review of this manuscript and approving it for publication was Byung-Seo Kim.

FIGURE 2. Growth of Blockchain technology for the insurance domain.

Existing solutions to address these challenges have been limited in scope and effectiveness. While some insurance companies have adopted digital technologies, such as mobile apps and online platforms, these solutions do not fully address the underlying issues of trust, security and efficiency. Moreover, the lack of interoperability among different insurance providers hinders the seamless exchange of information and collaboration.

To overcome these limitations, we propose a platform-agnostic framework that integrates blockchain technology and Internet of Things (IoT) for the insurance industry. Our framework aims to enhance transparency, security and customer experience by leveraging the benefits of blockchain's decentralized and immutable ledger, along with the real-time data capture capabilities of IoT devices. The key contributions of our work are as follows:

- A decentralized architecture that ensures trust and transparency among stakeholders
- Smart contract-based automation of insurance processes, including claim processing and settlement
- Integration of IoT devices for real-time data capture and risk assessment
- A platform-agnostic approach that enables interoperability and scalability

The rest of the paper is organized as follows: Section II provides a background on blockchain technology and its potential applications in the insurance industry. Section III discusses the existing insurance flow and the challenges it faces. Section IV introduces the architecture of the proposed blockchain-based insurance system, highlighting its key components and functionalities. Section V presents the results obtained from implementing the proposed framework, demonstrating its effectiveness in addressing the identified challenges. Section VI suggest possible workflows that can be implemented using the proposed system. Lastly, Section VII concludes the advantages of adopting a blockchain-enabled insurance system and discusses its potential future applications and scope.

II. BACKGROUND

A. MAPPING PAIN POINTS IN THE INSURANCE INDUSTRY TO BLOCKCHAIN OPPORTUNITIES

The insurance industry faces several significant pain points that hinder efficiency, security and customer satisfaction. As outlined in Fig. 3, these pain points include inefficient data exchange, high audit and redundancy needs, manual and laborious processes, complex assessment and governance, prone to fraud and data manipulation, multiple middlemen and data redundancy and fragmentation.

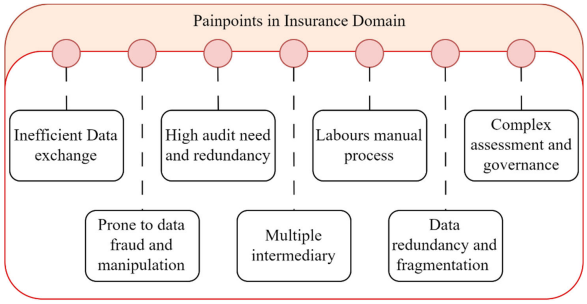


FIGURE 3. Painpoints of the insurance industry.

However, the emergence of blockchain technology offers promising solutions to address these challenges, as illustrated in Fig.4. By leveraging the opportunities provided by blockchain, the insurance sector can overcome its current limitations and create a more transparent, secure and efficient ecosystem.

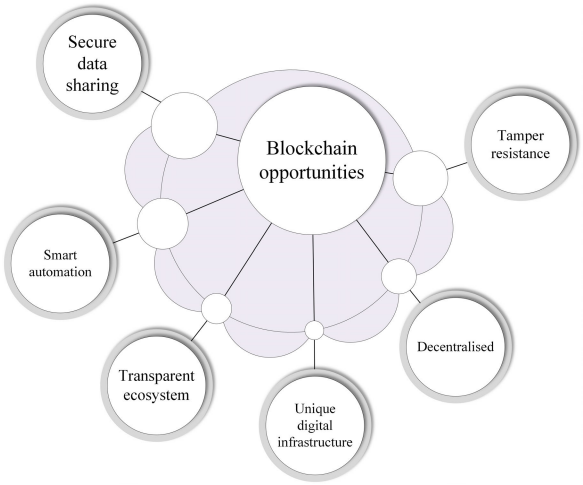


FIGURE 4. Blockchain opportunities in the Insurance domain.

Secure data sharing: Blockchain enables secure, tamper-proof data sharing among multiple parties, addressing the issue of inefficient data exchange and reducing the need for manual processes.

Tamper resistance: The immutable nature of blockchain records ensures that data cannot be altered or manipulated, mitigating the risk of fraud and enhancing trust among stakeholders.

Smart automation: Smart contracts on the blockchain can automate various processes, such as claims processing and policy enforcement, reducing the reliance on manual labor and increasing efficiency.

Decentralization: By decentralizing data storage and decision-making, blockchain eliminates the need for multiple intermediaries, streamlining operations and reducing costs.

Transparent ecosystem: Blockchain provides a transparent and auditable system, enabling all participants to access and

verify relevant information, thus reducing the complexity of assessment and governance.

Unique digital infrastructure: The blockchain network serves as a unified digital infrastructure, eliminating data redundancy and fragmentation and enabling seamless collaboration among stakeholders.

By mapping the pain points in the insurance industry to the opportunities offered by blockchain technology, it becomes evident that this innovative solution has the potential to revolutionize the sector. Embracing blockchain can lead to increased efficiency, enhanced security, reduced costs and improved customer experience, ultimately benefiting all stakeholders in the insurance ecosystem.

B. BLOCKCHAIN PENETRATION IN VARIOUS TYPES OF INSURANCE

Blockchain technology, coupled with IoT, has the potential to revolutionize the insurance industry by penetrating various verticals [3]. In the realm of term insurance, blockchain-based decentralized death registration have the potential to streamline records for government agencies and beneficiaries through the use of event-based smart contracts [4].

For motor insurance, blockchain can enhance product design, automate claims and facilitate end-to-end audits without the need for physical auditors, while also providing authorities and underwriters with rapid access to audit and process data due to its decentralized nature [5].

Fire insurance can benefit from IoT-enabled building management systems connected to a blockchain, which can accelerate accurate claim investigations and support for insurance agencies. This integration streamlines the registration, audit, evaluation and settlement processes for customers [6]. Within travel insurance, decentralized systems can enable real-time updates from airline industries to travel insurance providers, resulting in micro-level customized products for both insurers and customers [7].

Health insurance stands to gain from blockchain's ability to bring innovation and analytics-based patient coverage to health cases, aiding healthcare operators in eliminating overhead and expediting core processes [8].

Home insurance can leverage IoT-enabled smart homes connected to a blockchain ecosystem for real-time monitoring and log verification. This connection allows organizations to tailor products based on regional history and natural settings, ultimately providing customers with the advantage of automatic coverage [9].

C. INSURANCE DOMAIN THAT CAN BE BLOCKCHAIN AND IOT ENABLED

While all insurance types can benefit from blockchain integration, the degree of adaptability to IoT varies across domains [10]. Fig. 5 Notably, home and motor insurance have a higher potential for IoT adoption due to the increasing prevalence of smart home setups and connected intelligent car infrastructure. By embracing the blockchain IoT ecosystem, these two domains can pave the way for a more autonomous insurance process.

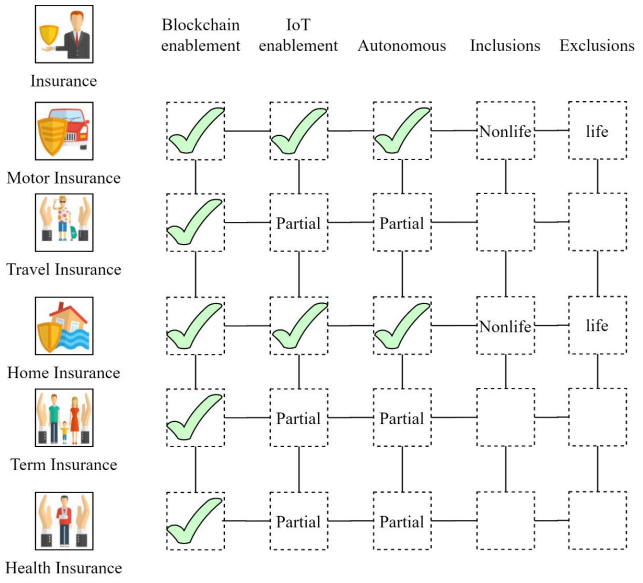


FIGURE 5. Blockchain IoT enablement for various insurance types.

D. POSSIBLE USE CASE SCENARIOS OF INSURANCE APPLICATIONS OF BLOCKCHAIN

Dynamic insurance: Enabled by blockchain's ability to maintain a full transaction history, real-time usage-based insurance reduces operational costs and preserves transaction data for future use [11]. Claim processing and subrogation: Smart contracts can simplify and automate these processes, making them less time-consuming [12]. Autonomous claim settlement: IoT-enabled devices can trigger loss notifications and invoke smart contracts in the blockchain ecosystem to process claim settlements without human intervention [13] and in similar lines used for agriculture insurance [14]. Reinsurance: Blockchain's timestamp-based and immutable records enable reinsurers to verify and approve claims more efficiently, avoiding time-consuming manual processes [15]. Fraud prevention: Blockchain-based systems protect information sharing and prevent data manipulation, reducing fraudulent claims and accelerating genuine claim settlement [16], [17].

E. VARIOUS TRANSACTIONS IN INSURANCE POLICY AND THE APPLICATION OF BLOCKCHAIN TECHNOLOGY

New Business: Insurer and policyholder sign a new insurance policy for a specified term. Blockchain can be used to implement a new business smart contract, streamlining the process [18], [19].

Endorsement: Any changes to an insurance policy are termed endorsements. Financial endorsements impact the premium and sum insured, while non-financial endorsements don't. Blockchain can be used to implement endorsement

smart contracts for both financial and non-financial scenarios [20], [21].

Renewal: When a policy term ends, it can be renewed for the next year with the same benefits and coverage. Blockchain can be used for renewal smart contracts [22].

Cancellation: An existing insurance policy can be cancelled by the insured or insurer and blockchain can be used to implement cancellation smart contracts [23].

Reinstatement: Cancelled policies can be reinstated upon request from the insured, with the same benefits and coverage. Blockchain can be used for reinstatement smart contracts [24], [25].

III. LITERATURE REVIEW AND EXISTING WORKFLOW IN THE INSURANCE INDUSTRY

Based on the generalized keywords, we can identify several important themes related to the use of blockchain in the insurance industry. One theme is the potential for blockchain to improve productivity and reduce complexity in insurance processes. Several studies have found that blockchain can serve as a single source of truth, leading to increased efficiency and transparency in insurance operations [20].

Another important theme is the potential for blockchain to enhance the financial security of insurance schemes. One study focused on the National Health Insurance Scheme (NHIS) in Ghana and found that blockchain-based solutions could help protect the scheme from financial problems caused by fraud and other data-related issues [20].

Additionally, blockchain technology can provide increased privacy and security in insurance processes, such as in the case of insurance claim management. Several studies have explored the use of zero-knowledge proof technology and smart contracts to protect the privacy and legitimacy of medical data in insurance claims [8].

Other themes include the use of blockchain in cryptocurrency mining, risk sharing and ruin theory [27], as well as the use of blockchain in healthcare 4.0 and electronic health record (EHR) management [30]. Overall, the use of blockchain technology in the insurance industry has the potential to improve efficiency, security and privacy in insurance processes.

Having a platform-agnostic blockchain framework for insurance applications is important because it allows for greater interoperability and flexibility in implementing blockchain solutions across different insurance providers and systems [19]. By using a standardized blockchain framework, insurance companies can avoid the need to develop custom solutions and can instead focus on integrating with existing blockchain platforms.

A platform-agnostic blockchain framework also enables greater collaboration and information sharing between insurance companies, regulators and other stakeholders. This can lead to a more robust and secure insurance ecosystem, where data and information can be shared safely and efficiently [19].

Furthermore, a platform-agnostic blockchain framework can reduce the costs and risks associated with implementing blockchain solutions. By using a standardized framework, insurance companies can take advantage of existing tools and resources, rather than investing in costly custom solutions. This can also help reduce the risk of errors and vulnerabilities that may arise from proprietary solutions [19].

Based on the consolidation of Table 1 and Table 2, it is evident that blockchain has the potential to revolutionize the insurance domain by improving security, transparency and efficiency in various processes. However, further research is necessary to identify and address the challenges that impede the adoption of blockchain in the insurance industry. Some of the potential research directions include developing regulatory frameworks, enhancing interoperability between different blockchain platforms and exploring the potential of emerging technologies such as zero-knowledge proofs and semantic web technologies in insurance applications. Additionally, research could focus on developing incentive models for incentivizing insurance companies to adopt blockchain technology and evaluating the social and economic impact of blockchain on the insurance industry.

IoT and Blockchain have a blended contribution in most application domains. The rising importance is emphasized by [31], which discusses how blockchain can secure IoT devices. [32] presents Physical Unclonable Function (PUF) for PUF-based Device Identity Management (PUF-DIM), a technique that has potential for repurposing in various avenues of Blockchain and IoT-based applications. PUF-DIM leverages the unique physical characteristics of IoT devices to generate secure and tamper-proof identities, which can be integrated with blockchain technology to enhance security, authenticity and trust in IoT ecosystems.

Developing a platform-agnostic blockchain framework for insurance applications is essential for realizing the full potential of blockchain technology in the insurance industry. It enables interoperability between different blockchain platforms and facilitates seamless data exchange between insurance companies, policyholders and other stakeholders. It also reduces the costs and complexities associated with developing and maintaining proprietary blockchain solutions. Moreover, a platform-agnostic blockchain framework promotes innovation and competition among different blockchain platforms, leading to better solutions for the insurance industry. Therefore, it should be a priority for researchers and developers working on blockchain applications for the insurance domain.

A. EXISTING WORK FLOW IN INSURANCE INDUSTRY

Fig. 6 presents the existing workflow of the insurance industry. The conventional actors present in the workflow are the Claims capturing system with a support team and Assessor with various administrative roles. The basic one is the claim investigation role, followed by claim estimation. The mature or final authority would be the chief assessor team that appraises, audits and approves the initiated claim. The approved claim goes to the settlement team, verifies the

TABLE 1. Literature review on blockchain in insurance industry.

Ref	Contribution to Insurance Domain	Blockchain to Achieve the Contribution
[26]	Finding potential opportunities for the insurance sector on the implementation of blockchain technology	Blockchain technology used as a single source of reality to improve productivity and mitigate complexity of insurance processes
[20]	Design and implementation of a blockchain-based solution to protect the National Health Insurance Scheme (NHIS) from plummeting financially	Cloud-based blockchain technology used to improve financial security of NHIS
[8]	Developing a distributed application using blockchain technologies that allows individuals and health insurance organizations to come into agreement during the implementation of healthcare insurance policies	Blockchain and semantic web technologies used for the formal expression of insured individual's data and contract terms
[27]	Investigating to what extent it is of interest to join a mining pool that reduces the variance of the return of a miner for a specified cost for participation using methodology from ruin theory and risk sharing in insurance	Quantitative study of effects of pooling in the context of blockchain mining in pools
[28]	Proposing a novel medical insurance claim scheme based on smart contracts, blockchain and zero-knowledge proof for ensuring the privacy and authenticity of patients' medical data in the medical insurance claim process	Zero-knowledge proof technology used to ensure the privacy and authenticity of patients' medical data in the medical insurance claim process
[29]	Designing a system by using UML diagram and simulating the use of DApps offered by the Vexanium Ecosystem to integrate blockchain for health insurance in Indonesia with hash authentication	UML diagram and DApps used to integrate blockchain for health insurance in Indonesia with hash authentication
[19]	Analysing how blockchain might reshape the insurance industry from an economic and business perspective and identifying challenges and enablers that specifically affect blockchain adoption within this industry through a Systematic Literature Review (SRL)	SRL used to identify challenges and enablers affecting blockchain adoption within the insurance industry
[30]	Developing an Ethereum blockchain-based framework, ChainSure, to provide an automated, tamperproof, transparent, scalable system for healthcare insurance management	Ethereum blockchain-based framework, ChainSure, used to provide an automated, tamperproof, transparent, scalable system for healthcare insurance management

TABLE 2. Existing work contribution across generalised category.

#	Blockchain Technology	Insurance Industry	Financial Security	Productivity	Privacy and Security
[26]	x	x		x	
[20]	x		x		x
[8]	x	x			x
[27]	x		x		x
[28]	x	x			x
[29]	x	x		x	x
[19]	x	x	x	x	
[30]	x	x	x		x

beneficiary's details and process the payment via the financial institution. As observable, the conventional process involves many teams, manual process and multiple institutions. These manual processes create bottle neck and delay in the process. Though many software supports the insurance industry, they cannot operate autonomously. The following are the limitations and the need for an innovate solution.

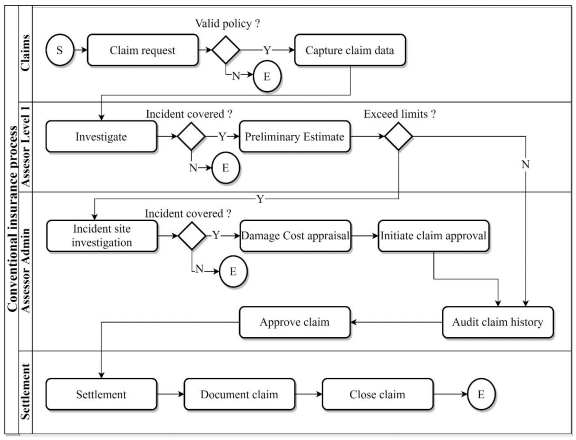


FIGURE 6. Workflow of a conventional insurance industry.

B. LIMITATIONS

Based on the Table 1 the consolidated list of limitations are as follows:

- Existing systems can only insure as a whole and provide an insurance claim as a whole.
- Insurance of individual items is not possible and not all providers support all household items and structures.
- The customer must find an insurer and service for each item separately and managing all the insurance and claim processes requires a lot of documentation and management.
- It requires expert actuators for every item involved to statistically analyse all the risks involved and it's a tedious process for insurance product design.
- Assessors with multiple skills are required and are bound to delay the process during calamities.
- Claim registration, processing, evaluation, payment approval and payout are monitored by humans, leading to human error, delays and overhead.

IV. PROPOSED SYSTEM

Insurance systems built on blockchain and an IoT-based ecosystem are large enterprise systems. The IoT sensor plays the important role of continuous monitoring and replaces

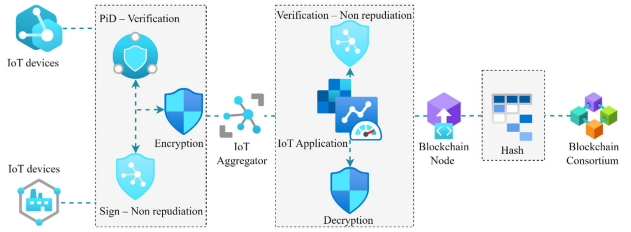


FIGURE 7. Novel infrastructure architecture for building insurance blockchain ecosystem based on [33].

the conventional auditing and verification process. The blockchain nodes serve as the nonmutable ledger, providing an uncompromised record and an audit log of all events in the ecosystem. An audit or origin assessment of data is an unachievable nightmare for system integrators in the vast ecosystem with millions of sensors working for a claiming process.

The full blockchain obtains updates across all nodes and remains the source of truth. When a system or a user wants to verify the origin of data, a verification request with a message tuple is sent to the blockchain node and routed to the aggregator, which in turn responds with TRUE or FALSE regarding the data origin question.

The insurance system uses the High-performance Edwards curve aggregate signature (HECAS) for non-repudiation and authentication. Elliptic Curve ElGamal(EC-EG) and Genetic Algorithm(GA)-based hash are used for security, privacy and block hashing. Designing a system based on the superior and proven method make the proposed framework novel and carry all the optimised advantage of the used methods. Fig. 7 represents infrastructure needs the proposed framework.

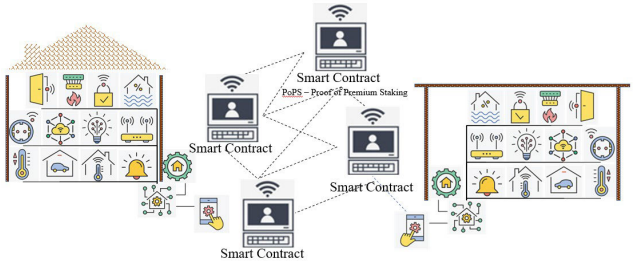


FIGURE 8. Aggregator high-level flow of proposed architecture [33].

Fig. 8 represents how the aggregator replies with a Boolean flag, which is redirected to the insurance team to reassure them and audit the authenticity of the data.

Table 3 presents the attribute level advantage of the novel proposed consensus that would be used for the insurance domain ecosystem.

Using the proposed framework, it's possible to implement parametric home insurance. A system, when designed using this framework, would contain an embedded contract with policy logic and a digital fee that would trigger it based on the IoT sensor installed with predefined logic and tamper-resistant physical identity (PiD). The settlement is autonomous as the trigger oracle is from per audited sensor. The triggered oracle is always authentic as long as the tamper flag of the PiD is FALSE. These can help streamline any insurance-linked securities to detailed customization.

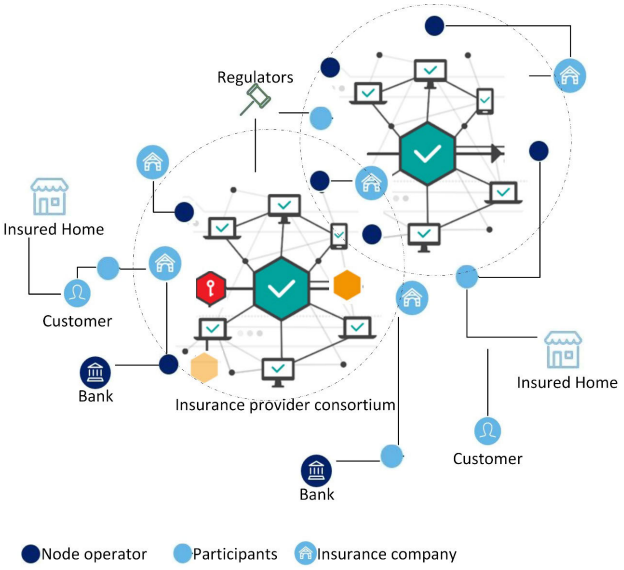


FIGURE 9. Participants - framework for platform agnostic blockchain IoT-based insurance solution.

Fig. 9 shows the proposed framework with two different ecosystems designed with enhanced security, hashing and high-performance signature based on EC-EG, Genetic Algorithm-Based SHA (GASHA) and HECAS. Let's assume the ecosystems are built on two different blockchain platforms. There are regulators, Insurance providers, Customers and banks in both ecosystems. Customers, when insuring a home product, subscribe to the SMART IoT monitoring solution that authentic parties can only provide. The IoT device, preinstalled with PiD, would connect autonomously with the ecosystem and continuously monitor the insurance product. The log is continuously pushed to the ecosystem, which forms a data pool for analytics. The tamper flag is on the loop check and when a tamper flag is raised, the system is expelled from the network automatically

A. PROPOSED ARCHITECTURE

This section details System flow, PiD, Consensus proofs, Validator selection mechanism and Model architecture framework for a platform-agnostic blockchain ecosystem designed specifically for the insurance industry.

Let's start by breaking down the system flow components and their roles in the system:

Datasource: This component represents the origin of data, which can come from various sources such as IoT sensors, aggregators and other relevant data points. Support Team: The support team assists in managing and maintaining the ecosystem, ensuring smooth operation and addressing any issues that may arise. API: The Application Programming

TABLE 3. Proposed consensus PoPS and PoTD.

Algorithm	Mining Power	MA	PaO	PrO	TPut	IoT Limitation
PoTD	Transaction density determines the miner in the consortium	Known	Low	Negligible	High	Reduce overhead, sorting and limit traffic.
PoPS	Large premium staked by the organization	Known	Low	Negligible	High	Reduce overhead, sorting and limit traffic.

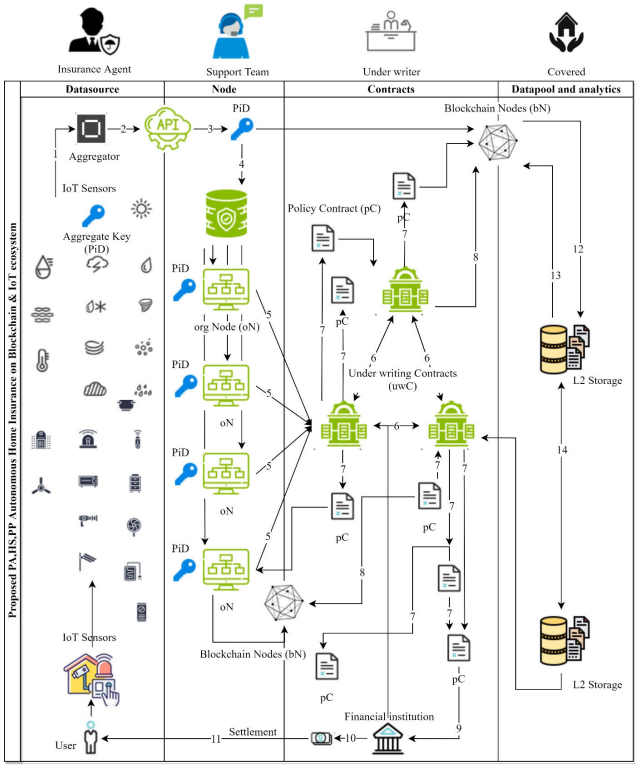


FIGURE 10. Detailed flow of proposed architecture for Insurance ecosystem.

Interface (API) acts as a bridge between the datasource and the blockchain nodes. It enables communication and data exchange between these components. PiD: The PiD (Physical Identity) is a unique identifier associated with each data point or transaction within the system. Blockchain Nodes (bN): These nodes form the core of the blockchain network. They are responsible for validating and storing transactions, as well as maintaining the integrity of the blockchain ledger. Policy Contract (pC): Smart contracts specific to insurance policies are deployed on the blockchain. These contracts automate the execution of policy terms and conditions, ensuring transparency and efficiency in the insurance process. Under writing Contracts (uwC): Similar to policy contracts, underwriting contracts are smart contracts that automate the underwriting process, assessing risk and determining policy premiums based on predefined rules and criteria. Covered: This component represents the entities or individuals covered under the insurance policies managed within the blockchain ecosystem. Under writer: Underwriters are responsible for assessing risk, determining policy terms and setting premiums for insurance policies. They interact with the blockchain ecosystem to automate and streamline the underwriting process. Financial Institution: Financial institutions, such as banks or insurance companies, are integrated into the ecosystem to facilitate financial transactions, premium payments and claims settlements. Settlement: The settlement process involves the resolution and payout of insurance claims. It is automated and executed through smart contracts on the blockchain, ensuring prompt and accurate settlements. L2 Storage: The system incorporates Layer 2 (L2) storage solutions to enhance scalability and efficiency. L2 storage allows for off-chain data storage while maintaining the security and integrity of the blockchain. The arrows in the Fig. 10 represent the flow of data and interactions between different components of the ecosystem. For example, data from IoT sensors is aggregated and passed through the API to the blockchain nodes. The nodes validate and store the data, triggering the execution of relevant smart contracts (policy contracts and underwriting contracts). The underwriters and financial institutions interact with the blockchain ecosystem to manage policies, assess risk and facilitate transactions.

The flow of the framework help to depict a transparent, efficient and secure blockchain-based ecosystem for the insurance industry, enabling streamlined processes, automated policy management and improved customer experiences.

1) PHYSICAL IDENTITY

The proposed framework introduces an IoT-enabled device for home insurance, revolutionizing the traditional claim process. Unlike conventional home insurance, where claims are typically made in full or only once without a system in place to claim individual items within the home, the PiD-enabled IoT device addresses this limitation. It enables an authentic, automated claim process, acting as a parametric model where each item is individually identified with a unique PiD [33].

When an insured clause is triggered, an auto claim is initiated. The initiation is verified with an analytical contract to determine the genuineness of the trigger. Based on the smart analytics contract, the smart settlement contract

then triggers the payment to be settled. This entire scenario operates autonomously, with the complete loop kept tamper-proof using PiD-enabled IoT devices, the HECAS signing and verification process and a privacy-protected blockchain ecosystem [28].

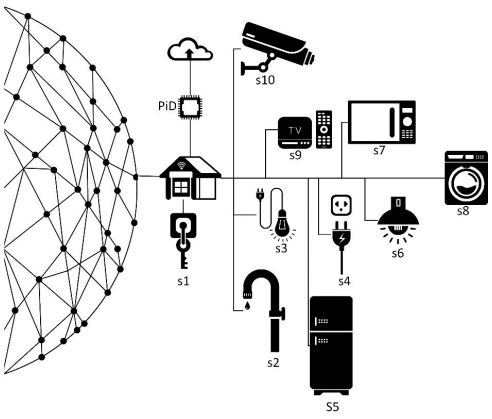


FIGURE 11. IoT-enabled SMART home depicting PiD and Sensors.

Fig. 11 illustrates an example of an IoT-enabled smart home setup, where various devices are labeled as follows: S_1: Smart lock, S_2: Smart water faucets, S_3: Smart lighting system, S_4: Smart plugs, S_5: Smart refrigerator, S_6: Smart exhaust, S_7: Smart oven, S_8: Smart washing machine, S_9: Smart TV and S_{10}: Smart security camera.

All these smart devices are initialized with PiD, allowing insurance providers, authentic service providers and regulators to identify each device individually. The novel PiD enables IoT devices to securely connect to the blockchain ecosystem and eliminates malicious devices from gaining access to the ecosystem [26].

Fig. 10 and Fig. 11 depict the detailed flow of the proposed architecture for the Insurance ecosystem and an IoT-enabled SMART home, respectively, illustrating the integration of technology in enhancing traditional insurance models.

The proposed IoT-enabled home setup with PiD offers numerous advantages over traditional home insurance systems. By facilitating the identification and claiming of individual items, it provides a more granular and accurate approach to insurance coverage. The automated claim process, supported by smart contracts and the blockchain ecosystem, ensures a tamper-proof and efficient settlement of claims [27].

Furthermore, the integration of PiD-enabled IoT devices boosts the security and reliability of the system by preventing unauthorized access and ensuring that only genuine devices are connected to the blockchain network. This novel approach to home insurance leverages the power of IoT and blockchain technologies to create a transparent, secure and customer-centric insurance ecosystem [30].

Recognition and Authentication Each PiD is associated with a unique identifier, ID_i, which is mathematically generated using a cryptographic hash function H. The hash function ensures that each IoT device's identifier is unique and tamper-evident. The recognition and authentication process can be represented as:

$$ID_i = H(\text{Device}_{\text{parameters}} \parallel \text{Secret}_{\text{key}})$$

where $\parallel$ denotes concatenation, $\text{Device}_{\text{parameters}}$ include the device's physical and operational characteristics and $\text{Secret}_{\text{key}}$ is a cryptographic key unique to each device, ensuring the ID_i's uniqueness and security.

Proving Non-Repudiation Non-repudiation ensures that a device cannot deny its actions or transactions. This is achieved through digital signatures, where each device has a pair of keys: a private key (K_{private}) and a public key (K_{public}). When a device sends data or performs an action, it signs the message with its K_{private}. The signature, Sig, can be expressed as:

$$Sig = \text{sign}(K_{\text{private}}, \text{Data})$$

Any party with the device's K_{public} can verify the signature, thus ensuring non-repudiation. The verification function is:

$$\text{verify}(K_{\text{public}}, Sig, Data) = \begin{cases} \text{True, if } Sig \text{ is valid} \\ \text{False, otherwise} \end{cases}$$

Ensuring Uniqueness To ensure that each device in the network is unique and cannot be duplicated, a registration mechanism is employed where the device's ID_i and K_{public} are registered in the blockchain. The registration can be represented as a transaction, Tx_{register}:

$$Tx_{\text{register}} = \{ID_i, K_{\text{public}}\}$$

The blockchain ensures immutability and transparency, making it computationally infeasible for any entity to duplicate or forge the identity of an IoT device within the ecosystem.

Scalability of IoT Devices The scalability of PiD to accommodate rapid growth of IoT devices in a blockchain ecosystem is facilitated by the efficient signature generation and verification attribute of HECAS. The blockchain acts as a decentralized ledger that records all Tx_{register} transactions, ensuring that each device's identity is securely and uniquely stored. The use of HECAS ensures that the system can handle a large scale of devices without compromising security or performance.

2) CONSENSUS

In blockchain technology, consensus refers to the mechanism by which all participants in a decentralized network agree on the validity and order of transactions, ensuring the integrity and security of the shared ledger. Consensus algorithms play a crucial role in maintaining the trustworthiness and immutability of the blockchain, preventing double-spending and resolving conflicts among participants.

Traditional consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), have been widely used in various blockchain networks. However, these mechanisms

may not always align with the specific requirements and characteristics of certain industries, such as the insurance sector. To address this, industry-specific consensus mechanisms have been proposed to better suit the needs and incentives of participants within those particular domains.

Proof of Premium Staking and Proof of Transaction Density are two such consensus mechanisms designed specifically for the insurance industry.

Proof of Premium Staking (PoPS): PoPS is a consensus mechanism that leverages the existing concept of insurance premiums. In this approach, insurance companies or nodes stake a portion of their collected premiums as collateral to participate in the block creation process. The selection of the block forger is based on the ''premium age,'' which takes into account the number of premiums staked and the duration of the staking. This mechanism incentivizes insurance companies to stake more premiums for a longer period, as it increases their chances of being chosen as the forger and earning rewards. PoPS ensures that participants have a vested interest in the network's security and stability, as their staked premiums are at risk if they act maliciously. Proof of Transaction Density (PoTD): PoTD is another consensus mechanism tailored to the insurance industry, which selects the block forger based on the transaction density of participating insurance organizations. Transaction density refers to the number of transactions processed by an organization within a specific time unit (e.g., day, week, month). In PoTD, insurance organizations that process a higher volume of transactions have a higher probability of being selected as the forger. This mechanism encourages insurance companies to actively utilize the blockchain network for their operations, leading to increased adoption and real-world usage of the technology in the insurance sector. PoTD rewards organizations that contribute more to the network's activity and throughput, promoting a fair and efficient consensus process. The introduction of Proof of Premium Staking and Proof of Transaction Density as industry-specific consensus mechanisms addresses the unique challenges and requirements of the insurance sector. By aligning the incentives of participants with the network's goals and leveraging the inherent characteristics of the insurance industry, these mechanisms aim to foster trust, security and active participation within the blockchain ecosystem. As the insurance industry explores the potential of blockchain technology, the development and implementation of tailored consensus mechanisms will play a vital role in driving adoption and unlocking the benefits of decentralized systems.

3) PROOF OF PREMIUM STAKING

Proof of Premium Staking is a consensus mechanism designed specifically for the insurance industry. It is based on the concept of staking insurance premiums to participate in the block creation process on a blockchain network. In this mechanism, insurance companies or nodes stake their collected premiums to earn the right to forge new blocks and receive rewards.

Algorithm 1 Proof of Premium Staking

```
function PremiumSelector
Input: header (prev hash, time stamp, address of node), nonce, threshold value, forger pool
Output: Fixed size valid block hash: (hash) premium age (node a)
    n ← number of premium staked (node a)
    premiumAccumulationTime ← number of days premium staked (node a)
    age ← n × premiumAccumulationTime
    return age
     Broadcast (header (prev block hash, time stamp, address of node), threshold value)
    for all staker i in staker pool do
         Compute blockHash ← SHA-GA(blockHeader (prev block hash, time stamp, address of node - e_i), nonce)
        if premiumAge(i) < thresholdValue then
            return False
        else
             Write block into blockchain
            return True
        end if
    end for
end function
```

The algorithm 1 represents the Proof of Premium Staking consensus mechanism for selecting a forger in a blockchain network specific to the insurance industry.

The PremiumSelector function takes the following inputs: Block header: previous block hash, timestamp and address of the node Nonce value Threshold value Forger pool (list of potential forgers) The function outputs a fixed-size valid block hash, which includes the hash and the premium age of the selected forger (node a). The premium age of node a is calculated as follows: n represents the number of premiums staked by node a. premiumAccumulationTime represents the number of days the premiums have been staked by node a. The premium age (age) is calculated by multiplying n and premiumAccumulationTime. The function returns the calculated premium age. The block header (previous block hash, timestamp, address of the node) and the threshold value are broadcast to the network. The algorithm iterates over each staker i in the staker pool (list of potential forgers). For each staker i, the block hash is computed using the SHA-GA algorithm. The inputs to the SHA-GA algorithm are: Block header: previous block hash, timestamp and address of the $node - e_i$ (the staker's identifier) Nonce value The computed block hash is compared against the threshold value: If the premium age of staker i is less than the threshold value, the function returns False, indicating that the staker is not selected as the forger. If the premium age of staker i is greater

TABLE 4. Working of Proof of Premium Staking (PoPS) and Proof of Transaction Density (PoTD).

Aspect	Proof of Premium Staking (PoPS)	Proof of Transaction Density (PoTD)
Concept	Staking insurance premiums as collateral for block creation	Selecting forger based on transaction density of insurance organizations
Staking Mechanism	Insurance companies stake a portion of collected premiums	No staking required
Forger Selection	Based on "premium age" (number of premiums staked × staking duration)	Based on transaction density (transactions processed per time unit)
Incentivization	Encourages long-term staking of premiums for higher chances of being selected as forger	Encourages active participation and high transaction throughput
Network Security	Staked premiums act as collateral, discouraging malicious behavior	Relies on the assumption that organizations with high transaction density are trustworthy
Rewards	Forgers earn rewards for creating blocks (transaction fees and/or newly minted tokens)	Forgers earn rewards for creating blocks (transaction fees and/or newly minted tokens)
Alignment with Insurance Industry	Leverages the concept of insurance premiums, which is familiar to industry participants	Focuses on transaction volume, which is a key metric in the insurance industry
Fairness	Favors participants with larger premium stakes and longer staking durations	Favors participants with higher transaction processing capabilities
Adoption	Encourages insurance companies to stake premiums and participate in the network	Encourages insurance companies to actively use the blockchain network for their operations
Real-World Usage	Promotes long-term commitment to the network through premium staking	Promotes real-world usage of the blockchain network in the insurance sector

than or equal to the threshold value, the block is written into the blockchain and the function returns True, indicating that the staker is selected as the forger. The iteration continues until a staker is selected as the forger or all stakers in the pool have been evaluated. The Proof of Premium Staking algorithm selects a forger based on their premium age, which is calculated by multiplying the number of premiums staked and the duration of the staking. The staker with a premium age greater than or equal to the threshold value is chosen as the forger. This mechanism incentivizes insurance companies to stake more premiums for a longer duration to increase their chances of being selected as the forger.

The algorithm ensures that the forger selection process is based on the commitment and stake of the participants in the insurance-specific blockchain network, promoting fairness and encouraging active participation.

4) PROOF OF TRANSACTION DENSITY

Proof of Transaction Density is a consensus mechanism designed for blockchain networks in the insurance industry. It aims to select the block forger based on the transaction density of insurance organizations participating in the network. Transaction density refers to the number of transactions processed by an insurance organization within a specific time unit (e.g., day, week, month).

The TransactionDensitySelector function in algorithm 2 takes the block header (previous hash, timestamp, address of node), nonce, threshold value and forger pool as input. It calculates the transaction density for the insurance organization (node a) by dividing the number of transactions processed (n) by the time unit (timeUnit), which can be a day, week, month, or any other relevant time period. The transaction density is returned. The block header and threshold value are broadcast to the network. For each insurance organization i in the forger pool: The block hash is computed using the SHA-GA algorithm, taking the block header (previous hash, timestamp, address of $node - e_i$) and nonce as input. If the transaction density of organization i is less than the threshold value, the function returns False. Otherwise, the block is written into the blockchain and the function returns True. The process continues for each organization in the forger pool. This algorithm selects the insurance organization with a transaction density above the specified threshold value to forge the next block in the blockchain. The organization

Algorithm 2 Proof of Transaction Density

```
function TransactionDensitySelector
Input: header (prev hash, time stamp, address of node), nonce, threshold value, forger pool
Output: Fixed size valid block hash: (hash) transaction density (node a)
    n ← number of transactions processed (node a)
    timeUnit ← time unit (e.g., day, week, month)
    density ← n/timeUnit
    return density
     Broadcast (header (prev block hash, time stamp, address of node), threshold value)
    for all organization i in forger pool do
        Compute blockHash ← SHA-GA(blockHeader (prev block hash, time stamp, address of node - e_i), nonce)
        if transactionDensity(i) < thresholdValue then
            return False
        else
            Write block into blockchain
            return True
        end if
    end for
end function
```

with a higher transaction density is more likely to be chosen as the forger, incentivizing organizations to process more transactions and maintain a high level of activity within the network.

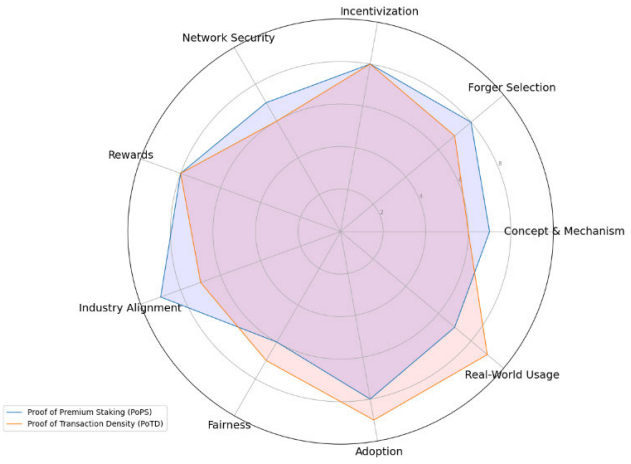


FIGURE 12. Comparison of Proof of Premium Staking (PoPS) and Proof of Transaction Density (PoTD).

Fig. 12 visually encapsulates the strengths and weaknesses of each consensus mechanism, offering insights into how they cater to the insurance industry's needs.For comparing Proof of Premium Staking (PoPS) and Proof of Transaction Density (PoTD) across various aspects such as concept and mechanism, forger selection, incentivization and more. Each aspect was rated on a scale from 1 to 10 based on its description, where a higher score indicates a stronger presence or emphasis in that category.

Concept and Mechanism: Reflects the foundational principles behind each protocol. PoPS has a slight edge due to its unique staking mechanism. Forger Selection: Indicates how each protocol selects entities for block creation. PoPS scores higher due to its premium age concept. Incentivization: Shows how each protocol encourages participation. Both protocols score high, reflecting their effective incentive mechanisms. Network Security: Assesses the security features of each protocol. PoPS is slightly favored due to its collateral-based security. Rewards: Looks at the reward system for forgers. Both protocols score equally, offering rewards for block creation. Industry Alignment: Evaluates how well each protocol aligns with the insurance industry. PoPS is seen as more closely aligned. Fairness: Considers how fair the protocol is towards participants of all sizes. PoTD is rated as slightly more fair due to its emphasis on transaction processing capabilities. Adoption: Reflects the potential for widespread use within the insurance industry. PoTD scores higher, suggesting greater ease of adoption. Real-World Usage: Measures the protocol's applicability to real-world operations. PoTD is seen as more practical for real-world usage.

5) VALIDATOR VOTING

Algorithm 3 presents the validator voting mechanism, which is responsible for selecting a validator to append a block to the blockchain.

The pickValidator function is defined. Mutation locks are enabled to prevent concurrent access to shared data. The function checks if the universal sleep time and lock time are active and assigns their values to local variables. Mutation locks are disabled. The function retrieves the temporary blocks from tempBlocks. An empty lottery array is initialized. The function checks if there are any temporary blocks, if all nodes are active and ready to participate in validation and if all participant flags are set to TRUE. If the conditions in step 7 are met, the function iterates over all validators. For each validator, it checks if a block has been submitted. If a block is submitted, the function considers either the transaction volume or the premium staked (depending on the specific implementation). The function iterates over all blocks in temp and all nodes in the lotteryPool. If the block's validator matches a node in the lotteryPool, the function continues to the next block. The function acquires a lock on the validatorsPoolLock. Mutation locks are enabled. The function retrieves the set of validators. Mutation locks are disabled. The function retrieves the number of times the block's validator appears in the setValidators. If the validator is found in setValidators, the function appends the block's validator to the lotteryPool k times. The function creates a new random source using the current time. It initializes a new random generator r using the random source. The function selects a lottery winner from the lotteryPool based on the comparison of the random value generated by r and the value of the premium (or transaction volume). The function iterates over all blocks in temp. If the block's validator matches the lottery winner, the function enables mutation locks, appends the block to the blockchain, disables mutation locks and announces the winning validator to all validators. It then breaks out of the loop. The function enables mutation locks, clears the tempBlocks array and disables mutation locks. The pickValidator function ends. This algorithm ensures that a validator is selected fairly based on the transaction volume or premium staked and the selected validator's block is appended to the blockchain. The use of mutation locks and random number generation adds security and randomness to the validator selection process.

6) MODEL ARCHITECTURE

The proposed model architecture presents Fig.13 a comprehensive solution for a platform-agnostic blockchain and IoT-based insurance system. By leveraging the strengths of both technologies, this model aims to revolutionize the insurance industry, offering enhanced efficiency, transparency and accessibility.

The architecture is composed of six interconnected modules, each serving a specific purpose:

Algorithm 3 Validator Voting Mechanism

```
function pickValidator
    Mutation.Lock.enable()
    check universal.Sleeptime.isActive
    assign local.Sleeptime = universal.Sleeptime
    check universal.Locktime.isActive
    assign local.Locktime = universal.Locktime
    Mutation.Lock.disable()
    temp ← tempBlocks
    lottery ← [ ]   ▷ check if all nodes are active and ready to participate in validation
    if len(temp) > 0 and allActive(temp) is TRUE and allParticipantFlag() is TRUE then
        for all validators do
            if isBlockSubmitted == TRUE then
                transactionVolume or premiumStaked
                for all blocks in temp do
                    for all node in lotteryPool do
                        if block.Validator == node then
                            continue
                        end if
                    end for
                    validatorsPoolLock
                    Mutation.Lock.enable()
                    setValidators ← validators
                    Mutation.Lock.disable()
                    k, ok ← setValidators[block.Validator]
                    if ok then
                        for i = 0tok − 1 do
                            lotteryPool.append(block.Validator)
                        end for
                    end if
                end for
            end if
        end for
        s ← pool.NewSource(time.Now())
        r ← pool.New(s)
        lotteryWinner ← lotteryPool[r.Compare((valOfPremium))]
        for all block in temp do
            if block.Validator == lotteryWinner then
                Mutation.Lock.enable()
                Blockchain.append(block)
                Mutation.Lock.disable()
                for all validator in validators do
                    announcements ← winning validator ← lotteryWinner
                end for
                break
            end if
        end for
    end if
    Mutation.Lock.enable()
    tempBlocks ← [ ]
    Mutation.Lock.disable()
end function
```

User Experience Module, composes the user interface, API integration and smart contracts for seamless policy handling, claims processing and underwriting. This module ensures a user-friendly experience while maintaining the security and integrity of the system.

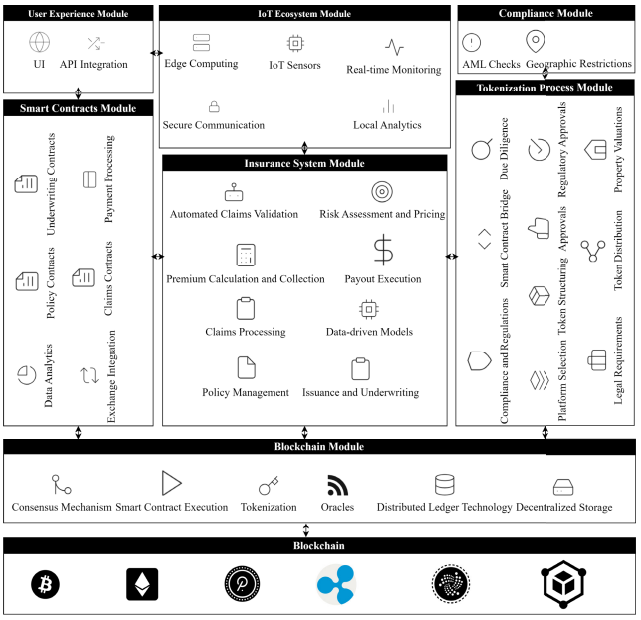


FIGURE 13. Model Architecture for a Platform-Agnostic Blockchain and IoT based Insurance System.

IoT Ecosystem Module, supports integrating edge computing, IoT sensors for real-time monitoring and secure communication protocols, this module enables the collection and processing of accurate, up-to-date data. This data is crucial for risk assessment and pricing, as well as for triggering automated actions based on predefined conditions.

Compliance Module, helps ensure regulatory adherence, the compliance module handles AML (Anti-Money Laundering) checks and enforces geographic restrictions. This module is essential for operating in different jurisdictions while maintaining legal compliance.

Tokenization Process Module, module facilitates the tokenization of insurance policies, enabling fractional ownership and increased liquidity. It encompasses various aspects such as smart contract bridging, legal requirements, underwriting approvals, regulatory valuations, token structuring and property valuations.

Insurance System Module, the core of the architecture, the insurance system module covers key functions such as automated claims validation, risk assessment and pricing, premium calculation and collection, payout execution, claims processing, data-driven models, policy management and issuance and underwriting. Automating these processes through smart contracts, the system becomes more efficient and transparent.

Blockchain Module, serves as the foundation and providing the necessary infrastructure for decentralization, security and immutability. It includes components such as consensus mechanisms, smart contract execution, tokenization, oracles

for external data feeds, distributed ledger technology and decentralized storage solutions.

The platform-agnostic nature of this architecture sets it apart. Designing the system to be compatible with various blockchain platforms, the model ensures flexibility and adaptability. This approach allows insurers to choose the blockchain platform that best suits their needs, considering factors such as scalability, interoperability and regulatory compliance.

Integration of IoT enables collection of real-time data from connected devices, wearable and sensors. This data can be used to customize insurance products, adjust premiums dynamically based on individual risk profiles and provide preventive recommendations to policyholders. The combination of IoT and blockchain technologies creates a powerful synergy, ensuring data integrity, privacy and security.

The proposed architecture also promotes the development of a decentralized marketplace for insurance products. By tokenizing insurance policies, the system enables the creation of a secondary market where policyholders can trade their tokenized assets. This feature provides increased liquidity and allows for the diversification of risk across a broader pool of investors.

The proposed platform-agnostic blockchain and IoT-based insurance system model offers a comprehensive and innovative approach to revolutionizing the insurance industry. Leveraging decentralization and immutability attribute of blockchain along with the real-time data collection IoT devices, enables the creation of a transparent, efficient and customer-centric insurance ecosystem. The platform-agnostic nature of this model ensures adaptability and compatibility across various blockchain platforms, providing flexibility for insurers to choose the most suitable infrastructure for their needs.

V. PROOFS, SECURITY, RESULTS AND DISCUSSION

A. PROOF OF CORRECTNESS

1) CORRECTNESS OF VALIDATOR VOTING MECHANISM

Assume a blockchain network with a set of nodes $\mathcal{N}$ and a subset $\mathcal{N}_v \subset \mathcal{N}$ consisting of validator nodes eligible to vote. Let $\mathcal{B}$ represent the set of all blocks that have been proposed for addition to the blockchain, with each block $b \in \mathcal{B}$ associated with a unique proposing validator node.

Define a weight function $w : \mathcal{N}_v \to \mathbb{R}^+$ which assigns a positive real weight to each validator node, representing the node's stake in the network. This weight could be a function of the node's staked tokens, its transaction volume, or other relevant measures of contribution to the network.

Definition 1 (Lottery Pool): A lottery pool $\mathcal{L}$ is a multiset where each validator node $n \in \mathcal{N}_v$ appears $w(n)$ times. The probability $P(n)$ of a validator node n being selected from $\mathcal{L}$ is proportional to its weight.

Theorem 1 (Fairness of Selection): The Validator Voting mechanism ensures that each validator node has a selection probability proportional to its weight, providing a fair chance of selection in the consensus process.

Proof: Let Ω be the sample space of all possible outcomes in the lottery draw. Each outcome $\omega \in \Omega$ corresponds to a draw from $\mathcal{L}$. The probability of a validator node n being selected is given by:

$$P(n) = \frac{w(n)}{\sum_{n' \in \mathcal{N}_v} w(n')}$$

Since the sum in the denominator is constant for a given round of selection, each node's probability is directly proportional to its weight, ensuring fairness.

Definition 2 (Random Selection Function): A random selection function select : $\mathcal{L} \to \mathcal{N}_v$ chooses a node from $\mathcal{L}$ based on a uniform random distribution.

Lemma 1 (Uniform Random Distribution): The selection function select induces a uniform random distribution over $\mathcal{L}$ if each node in $\mathcal{N}_v$ has an equal chance of being chosen per entry in the multiset.

Proof: Given the definition of $\mathcal{L}$, the function select will choose any single entry from $\mathcal{L}$ with equal probability. Since nodes may have multiple entries in $\mathcal{L}$, the total probability of selection for a node n is the sum of the probabilities of each of its entries, which by definition is $P(n)$.

Corollary 1 (Consensus Integrity): The consensus process retains its integrity under the Validator Voting mechanism, as the probability of a node's selection reflects its contribution to the network.

Proof: The probability of selection $P(n)$ serves as a measure of contribution. A consensus reached through such a mechanism is one that has considered the contributions of all participants fairly. Nodes with a higher stake and hence greater weight have a correspondingly higher chance to be selected, aligning their interests with the integrity of the network.

By employing a probability space and a random selection function that is uniform over the entries of the lottery pool, the Validator Voting mechanism achieves a fair and representative consensus process, integral to the security and reliability of the blockchain network.

2) INTEGRATED CORRECTNESS OF PROOF OF PREMIUM STAKING AND VALIDATOR VOTING MECHANISMS

In a blockchain system where validator selection is critical, the integration of the "Proof of Premium Staking" and "Validator Voting" mechanisms ensures a robust and equitable consensus model. We develop a mathematical framework that establishes the soundness and fairness of the integrated system.

Let $\mathcal{N}$ represent the set of all nodes within the blockchain network. Define two critical subsets of $\mathcal{N}$:

- $\mathcal{N}_s \subset \mathcal{N}$ where each node $n \in \mathcal{N}_s$ satisfies the staking condition defined by the "Proof of Premium Staking" mechanism, such that premiumAge$(n) \geq T$.
- $\mathcal{N}_a \subset \mathcal{N}$ where each node $n \in \mathcal{N}_a$ is active and eligible to participate as per the "Validator Voting" mechanism.

Definition 3 (Composite Eligibility Set): The composite eligibility set $\mathcal{N}_c$ is the intersection of $\mathcal{N}_s$ and $\mathcal{N}_a$:

$$\mathcal{N}_c = \mathcal{N}_s \cap \mathcal{N}_a$$

This set represents nodes that are both staking and active, qualifying them for the validation process.

Lemma 2 (Eligibility Invariant): For every consensus round, the eligibility of nodes is invariant to the selection process, meaning that $\mathcal{N}_c$ is fixed during a single round of validation.

Proof: Given the definitions of $\mathcal{N}_s$ and $\mathcal{N}_a$ and the assumption that T, the staking threshold and the state of node activity do not change during the selection process, $\mathcal{N}_c$ remains constant for that duration.

Theorem 2 (Fair Selection Probability): The probability of any eligible node n in $\mathcal{N}_c$ being selected in the lottery is proportional to its stake weight $w(n)$, which is a function of the node's transaction volume or premium staked.

Formally, for node $n \in \mathcal{N}_c$, the selection probability $P(n)$ is:

$$P(n) = \frac{w(n)}{\sum_{n' \in \mathcal{N}_c} w(n')}$$

This defines the fairness of the lottery draw.

Proof: The Validator Voting mechanism describes a process where each eligible node is entered into the lottery pool a number of times proportionate to its weight. This procedure ensures that the probability of selection for any node is fair and in direct relation to its contribution to the network.

Theorem 3 (Validator Selection Completeness): Given the probability distribution over $\mathcal{N}_c$, the selection process is complete, ensuring that every node in $\mathcal{N}_c$ has a non-zero probability of selection, assuming all $w(n) > 0$.

Proof: As $P(n) > 0$ for all $n \in \mathcal{N}_c$ with $w(n) > 0$ and since the lottery system is used for selection, the process is guaranteed to result in a selection from $\mathcal{N}_c$.

Corollary 2 (Robust Consensus Formation): The consensus formed via the integrated mechanism is robust, as it relies on the collective and weighted contribution of the most committed and reliable set of validators.

Proof: Since $\mathcal{N}_c$ represents a set of validators committed both by premium age and activity, the selection of any node n from $\mathcal{N}_c$ for block validation is representative of a consensus formed by committed validators.

we demonstrate that the integration of Proof of Premium Staking and Validator Voting results in a consensus algorithm that is sound in its selection of validators and equitable in representing the stake and activity of nodes.

3) INTEGRATED CORRECTNESS OF PROOF OF TRANSACTION DENSITY AND VALIDATOR VOTING MECHANISMS

The "Proof of Transaction Density" algorithm ensures that nodes contributing to transaction processing are recognized and potentially prioritized in the consensus process. Combining this with the "Validator Voting" mechanism, we establish a multifaceted approach to validator selection that considers both stake and transactional activity.

Definition 4 (Transaction Density): Let $\mathcal{T}_a$ represent the total number of transactions processed by node a in a given time unit τ (e.g., day, week, month). The transaction density $\delta(a)$ for node a is defined as:

$$\delta(a) = \frac{\mathcal{T}_a}{\tau}$$

Lemma 3 (Eligibility Based on Transaction Density): A node a is eligible for selection if its transaction density $\delta(a)$ exceeds a predefined threshold θ, i.e., $\delta(a) > \theta$.

Theorem 4 (Enhanced Fairness through Integrated Selection): The integration of the "Proof of Transaction Density" and "Validator Voting" mechanisms ensures that the probability of a node's selection not only reflects its stake but also its active contribution to network transaction processing.

Proof: Define $\mathcal{N}_d$ as the set of nodes whose transaction density exceeds θ. The intersection $\mathcal{N}_c \cap \mathcal{N}_d$ identifies nodes that are both staking significantly and actively processing transactions. A weighted selection mechanism is applied where weights consider both the stake (from "Validator Voting") and transaction density. Let $w'(n)$ represent this composite weight for node n. The probability $P'(n)$ of node n being selected is then proportional to $w'(n)$, ensuring fairness and rewarding network contributions:

$$P'(n) = \frac{w'(n)}{\sum_{n' \in \mathcal{N}_c \cap \mathcal{N}_d} w'(n')}$$

Corollary 3 (Network Efficiency and Security): By prioritizing nodes with higher transaction densities, the network not only rewards nodes that contribute to its efficiency but also enhances security by promoting the diversity of validators based on their active participation.

Proof: Nodes with higher transaction densities are more likely to have recent and frequent interactions with the network, indicating a vested interest in its integrity. This diversity in validator selection criteria reduces the risk of centralized control or manipulation.

Corollary 4 (Adaptive Network Evolution): The integrated mechanism allows the network to adaptively evolve by dynamically responding to changes in node behavior, transaction volume and network participation.

Proof: As transaction patterns and node participation evolve, the integrated selection criteria automatically adjust the eligibility and weighting of nodes for validator selection, ensuring that the network remains robust against a changing environment.

By mathematically formalizing the integration of "Proof of Transaction Density" with "Validator Voting," we demonstrate that the combined mechanisms significantly enhance the fairness, security and efficiency of the consensus process. This integrated approach ensures that validator selection is

not only based on stake but also on meaningful contributions to the network's operational efficiency.

B. SECURITY

Comparing the security of different consensus mechanisms can be complex and multifaceted. We employee Formal verification and Game theroy based analysis.

1) FORMULATION BASED ON FORMAL VERIFICATION

We employee Formal Verification consensus mechanisms have been subject to formal verification methods to assess their security properties rigorously. While this approach may not be feasible for every mechanism, it can provide strong evidence of security guarantees for those that have undergone such analysis.

a: FORMAL VERIFICATION FOR PROOF OF WORK (PoW)

MODELING COMPUTATIONAL POWER DISTRIBUTION

Let P_i represent the computational power of miner i in the network, where $i = 1, 2, \ldots, n$. Let T be the total computational power in the network, i.e., $T = \sum_{i=1}^{n} P_i$.

PROBABILITY OF WINNING

The probability of a miner winning the right to add the next block to the blockchain is proportional to their computational power. For miner i, the probability of winning is P_i/T.

51% ATTACK PROBABILITY

A 51% attack occurs when a single entity controls more than 50% of the total computational power. The probability of a successful 51% attack can be calculated as the cumulative probability of miners with more than 50% of the total computational power.

FORMAL VERIFICATION

Using mathematical models, probability theory and computational analysis, we can formally verify whether it is feasible for an attacker to accumulate more than 50% of the total computational power and execute a successful 51% attack. This analysis involves assessing the cost and feasibility of acquiring the necessary computational power and the likelihood of succeeding in the attack given the network's current state.

b: FORMAL VERIFICATION FOR PROOF OF STAKE (PoS)

MODELING STAKE DISTRIBUTION

Let S_i represent the stake (number of coins) held by validator i in the network, where $i = 1, 2, \ldots, n$. Let T be the total stake in the network, i.e., $T = \sum_{i=1}^{n} S_i$.

PROBABILITY OF BEING SELECTED AS VALIDATOR

In PoS, validators are chosen to create new blocks based on their stake. For validator i, the probability of being selected as the block proposer is S_i/T.

51% ATTACK PROBABILITY

A 51% attack in PoS occurs when a single entity controls more than 50% of the total stake. The probability of a successful 51% attack can be calculated as the cumulative probability of validators with more than 50% of the total stake.

FORMAL VERIFICATION

Similar to PoW, formal verification for PoS involves assessing the feasibility and cost of accumulating more than 50% of the total stake and executing a successful 51% attack. This analysis considers economic incentives, game theory and the network's security mechanisms to determine the likelihood of a successful attack and the potential consequences for the network's security.

c: FORMAL VERIFICATION FOR PROOF OF PREMIUM STAKING (PoPS)

MODELING PREMIUM STAKE DISTRIBUTION

Let S_i represent the premium stake (amount of insurance premium staked) by organization i in the network, where $i = 1, 2, \ldots, n$. Let T be the total premium stake in the network, i.e., $T = \sum_{i=1}^{n} S_i$.

PROBABILITY OF BEING SELECTED AS MINER

In PoPS, miners (validators) are chosen to mine new blocks based on their premium stake. For organization i, the probability of being selected as a miner is S_i/T.

51% ATTACK PROBABILITY

A 51% attack in PoPS occurs when a single entity controls more than 50% of the total premium stake. The probability of a successful 51% attack can be calculated as the cumulative probability of organizations with more than 50% of the total premium stake.

FORMAL VERIFICATION

Formal verification for PoPS involves assessing the feasibility and cost of accumulating more than 50% of the total premium stake and executing a successful 51% attack. This analysis considers economic incentives, game theory and the network's security mechanisms to determine the likelihood of a successful attack and the potential consequences for the network's security.

2) FORMULATION BASED ON GAME-THEORETIC ANALYSIS

a: PROOF OF WORK (PoW)

In PoW, miners compete to solve cryptographic puzzles to validate transactions and add blocks to the blockchain. The probability of a miner successfully mining a block is proportional to their computational power relative to the total computational power of the network. A 51% attack occurs when a single entity controls more than 50% of the total computational power, enabling them to manipulate the blockchain's transaction history. Game theory models can

analyze the incentives of miners to cooperate or defect in the network and assess the likelihood of a successful 51% attack based on their strategies.

b: PROOF OF STAKE (PoS)

In PoS, validators are chosen to create new blocks based on their stake (number of coins) in the network. The probability of being selected as a validator is proportional to a validator's stake relative to the total stake in the network. A 51% attack in PoS occurs when a single entity controls more than 50% of the total stake, enabling them to manipulate the blockchain's transaction history. Game theory models can analyze the incentives of validators to cooperate or defect in the network and assess the likelihood of a successful 51% attack based on their strategies.

c: PROOF OF PREMIUM STAKING (PoPS)

In PoPS, organizations stake insurance premiums to participate in block creation. The probability of being selected as a miner is proportional to an organization's premium stake relative to the total premium stake in the network. A 51% attack in PoPS occurs when a single entity controls more than 50% of the total premium stake, enabling them to manipulate the blockchain's transaction history. Game theory models can analyze the incentives of organizations to cooperate or defect in the network and assess the likelihood of a successful 51% attack based on their strategies.

Let's formalize the game-theoretic analysis of Proof of Work (PoW), Proof of Stake (PoS) and Proof of Premium Staking (PoPS) using mathematical notation to assess the probability of a successful 51% attack on each consensus mechanism.

d: PROOF OF WORK (PoW)

Let p_i represent the computational power of miner i in the network, where $i = 1, 2, \ldots, n$. The probability of miner i successfully mining a block is p_i/T, where $T = \sum_{i=1}^{n} p_i$ is the total computational power in the network. A 51% attack occurs when a single entity controls more than 50% of the total computational power, i.e., when $\sum_{i=1}^{m} p_i > 0.5 \times T$ for some m. We can use game theory to model the strategies of miners and analyze the likelihood of a successful 51% attack based on their actions and incentives.

e: PROOF OF STAKE (POS)

Let s_i represent the stake (number of coins) held by validator i in the network, where $i = 1, 2, \ldots, n$. The probability of validator i being selected to create a block is s_i/T, where $T = \sum_{i=1}^{n} s_i$ is the total stake in the network. A 51% attack occurs when a single entity controls more than 50% of the total stake, i.e., when $\sum_{i=1}^{m} s_i > 0.5 \times T$ for some m. Using game theory, we can analyze the strategies of validators and assess the likelihood of a successful 51% attack based on their behavior and economic incentives.

f: PROOF OF PREMIUM STAKING (POPS)

Let r_i represent the premium stake (amount of insurance premium staked) by organization i in the network, where $i = 1, 2, \ldots, n$. The probability of organization i being selected as a miner is r_i/T, where $T = \sum_{i=1}^{n} r_i$ is the total premium stake in the network. A 51% attack occurs when a single entity controls more than 50% of the total premium stake, i.e., when $\sum_{i=1}^{m} r_i > 0.5 \times T$ for some m. By applying game theory, we can model the strategic interactions of organizations and analyze the likelihood of a successful 51% attack based on their decisions and incentives.

g: COMPARATIVE ANALYSIS

We can compare the probabilities of 51% attacks in PoW, PoS and PoPS by assessing the concentration of computational power, stake and premium stake required to achieve such attacks. Mathematical analysis, simulations and empirical studies can further quantify these probabilities and provide insights into the relative security properties of each consensus mechanism. The formulations provided above serve as a basis for analyzing the security properties of PoW, PoS and PoPS using game theory. Limitation in the analysis include not considering Economic incentives and examination of potential attack vectors specific to each consensus mechanism.

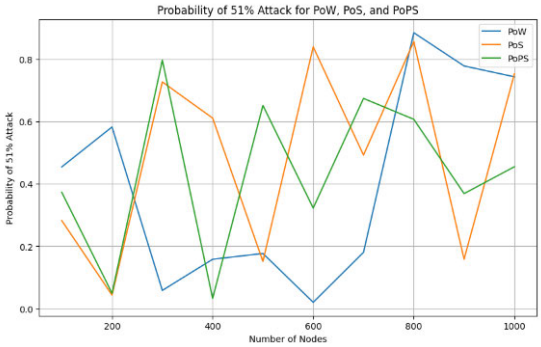


FIGURE 14. Probabilities of 51% attacks in PoW, PoS and PoPS.

The graph compares the probability of a 51% attack for three different consensus mechanisms: Proof of Work (PoW), Proof of Stake (PoS) and Proof of Premium Staking (PoPS) across varying numbers of nodes in a blockchain network.

As the number of nodes increases from 200 to 1000, the probability of a 51% attack decreases for all three consensus mechanisms. This trend demonstrates that a larger, more decentralized network is generally more resistant to 51% attacks, as it becomes increasingly difficult for an attacker to gain control over a majority of the network's resources.

However, there are notable differences in the attack probabilities among the three mechanisms:

Proof of Work (PoW) exhibits the highest probability of a 51% attack across all network sizes. Even with 1000 nodes, the probability remains above 20%. This vulnerability can be attributed to the resource-intensive nature of PoW, which allows attackers with significant computational power to

potentially dominate the network. Proof of Stake (PoS) shows a lower probability of a 51% attack compared to PoW. As the number of nodes increases, the probability decreases more rapidly, reaching around 10% at 1000 nodes. PoS relies on staked tokens rather than computational power, making it more challenging for attackers to acquire a majority stake. Proof of Premium Staking (PoPS) demonstrates the lowest probability of a 51% attack among the three mechanisms. The probability drops sharply as the network grows, at 1000 nodes. PoPS leverages the unique characteristics of the insurance industry, such as long-term staking of premiums, which further disincentivizes malicious behavior and enhances network security. The graph illustrates that while increasing the number of nodes improves security for all three consensus mechanisms, PoPS exhibits the strongest resistance to 51% attacks. This suggests that industry-specific consensus mechanisms, like PoPS for the insurance sector, can provide enhanced security by aligning incentives and leveraging domain-specific factors.

The graph highlights the importance of network decentralization and the potential benefits of tailored consensus mechanisms in mitigating the risk of 51% attacks. It underscores the need for careful consideration and selection of consensus mechanisms based on the specific requirements and characteristics of the industry or application.

C. SIMULATION RESULTS

Simulation of Validator Voting Mechanism mechanism with PoPS and PoTD.

Initialization and Assumptions Initialization: Create a list of validator nodes, each with properties like isBlockSubmitted, transactionVolume, premiumStaked and whether they are active and ready to participate. Define the universal properties like Sleeptime and Locktime, assuming these impact all validators equally. Initialize an empty list for tempBlocks and lotteryPool.

Function Behavior: The function pickValidator will simulate the selection of a validator to append a block to the blockchain. Implement helper functions like allActive(temp) to check if all nodes in tempBlocks are active and allParticipantFlag() to check if all conditions for participation are met.

Simulation Steps as follows, Locking Mechanism: Simulate enabling and disabling the mutation lock around critical sections to prevent race conditions. Validator Selection Process: Iterate over validators who have submitted blocks and populate the lotteryPool based on transactionVolume or premiumStaked. Winner Selection: Use a pseudo-random selection mechanism to pick a winner from the lotteryPool based on a comparison function (in this case, r.Compare((valOfPremium)) which we'll simulate as a random choice considering the valOfPremium). Block Appending: Append the block from the winning validator to the blockchain and announce the winning validator to all nodes. Cleanup: Clear the tempBlocks for the next round. Running the Simulation:Run the simulation multiple times with an increasing number of validator nodes to observe the mechanism's behavior and efficiency.In simulation version the transactionVolume and premiumStaked influence the likelihood of being chosen, without diving into complex real-world specifics.

1) SIMULATION A: PREMIUM STAKING

Demonstrates the fundamental operation of the algorithm, emphasizing the role of premiumStaked in influencing the selection process within the lottery pool. The random selection simulates the effect of various premiumStaked values, reflecting a basic version of the complex dynamics involved in a real-world validator voting mechanism.

The Blue line in Fig. 15 illustrates the effect of increasing the number of validators on the selection process, specifically showing the hypothetical premium staked values of the selected validators across different scenarios. As the number of validators increases, we observe the changes in the premium staked by the selected validator. This visualization aids in understanding how the selection dynamics might shift with the scale of participation, under the assumption that a validator's chance to append a block could be influenced by their premium staked.

2) SIMULATION B: TRANSACTION DENSITY

Simulation focusing on transaction density as the key factor for validator selection, we observed the following outcomes with an increasing number of validators. With 5 validators, it appears there were no eligible validators, which suggests that either no blocks were submitted by these validators or their transaction densities did not qualify them for the selection process in this specific run. With 10 validators, Validator 9 was successfully chosen to append a block, indicating a higher transaction density for this validator compared to others. Increasing the count to 20 validators, Validator 2 was selected for appending a block, further highlighting the influence of transaction density on the selection mechanism. This simulation underscores the impact of transaction density on the validator selection process, with those having higher transaction volumes being more likely to be chosen to append blocks. This mirrors real-world scenarios where validators with higher transaction activities might be preferred for certain tasks or rewards, aligning with the concept of Proof of Transaction Density.

The Red line in Fig. 15 illustrates the effect of increasing the number of validators on the selection process, with a focus on transaction density as the selection criterion. For the scenario with 5 validators, no selection was made due to eligibility issues, suggesting that transaction density or other qualifying factors were not met. As the number of validators increases, we see a rise in the transaction density of the selected validators, highlighting the role of transaction density in influencing the selection process. This visualization helps understand the dynamics of validator selection based on transaction activity, showing a preference for validators with higher transaction volumes as the network scales.

FIGURE 15. Comparison of premium staked and transaction density on the validator.

D. DISCUSSION

Premium Staked Stability and Long-Term Commitment: The premium staked criterion tends to favor validators who are willing to lock in significant resources for longer periods. This can enhance network security and stability, as validators have a vested interest in the network's integrity.

Threshold Barrier: There's a potential threshold barrier for new or smaller validators to become competitive, as larger validators with more substantial premium stakes might dominate the selection process.

Suitability: Best suited for networks seeking to incentivize long-term investment and commitment from its validators. It aligns well with scenarios where the size of the stake is directly correlated with trust and security, such as in financial or insurance-focused blockchains.

Transaction Density Activity and Participation: This criterion rewards validators based on their activity levels, encouraging frequent transactions and higher network participation.

Dynamic and Inclusive: It allows for a more dynamic selection process, potentially giving newer or smaller validators a chance to be selected if they can maintain a high level of activity.

Suitability: Ideal for networks aiming to maximize throughput and efficiency, or where transaction volume is a critical measure of participation and contribution. It encourages active network use and could promote scalability by incentivizing validators to process more transactions.

Conditions for Preference: Premium Staked is preferable in networks where the amount of stake signifies trustworthiness, financial commitment is crucial and where the goal is to ensure network security through substantial collateral. Transaction Density shines in scenarios where high throughput, scalability and active participation are valued over the financial size of the stake. It supports a more meritocratic approach, favoring validators who contribute significantly to network activity.

The choice between premium staked and transaction density as the basis for validator selection depends on the specific goals and characteristics of the blockchain network. For networks prioritizing security and stability through financial commitment, premium staked could be more advantageous. Conversely, for those focusing on network efficiency, throughput and inclusivity, transaction density offers a compelling criterion.

Table 5 presents the comparison of PoPS / PoTD with generic consensus its key inferences and discussions based on the comparison.

Each mechanism caters to different network philosophies and goals and the decision should align with the broader objectives of the blockchain ecosystem in question.

VI. WORKFLOW OF VARIOUS PROCESSES USING THE PROPOSED FRAMEWORK

The Blockchain Insurance Industry Initiative, is an international blockchain consortium aimed at streamlining workflows and processes in the insurance sector. Currently supporting over 40 companies, the initiative intends to bring significant benefits in the coming years. Key requirements specified to improve the industry include:

1) Enabling primary insurers, reinsurers, brokers and regulators to securely share data in real-time
2) Automating risk modeling, audits and compliance checks
3) Binding towers of risk and treaties on a single time-stamped smart contract
4) Streamlining workflow of high-value items and warrant tracking
5) Creating an immutable and trustworthy record of product provenance for the benefit of all stakeholders.
6) Tracking product ownership and claims in real-time, even across borders
7) Enhancing industry-wide efforts to mitigate claims fraud through superior data and data-sharing

The proposed framework consists of various types of smart contracts, as specified in Fig. 10, designed to address various core operations within the framework.

A. WORKFLOW OF KYC

Know your customer (KYC) is part of client onboarding and plays an important regulatory role in preventing anti-money laundering (AML). The corporate insurance industry operates in the conventional style, with a myriad of time-consuming procedures in place to fulfil KYC procedures, such as signature requirements, meeting face-to-face with clients and other manual processes. These methods are error-prone and inefficient. Due to regulatory concerns, financial institutions frequently do not share KYC. As a result, those who switch to a new provider for a better product or an uncovered feature will need to redo the same KYC process again. Finally, the manual KYC process is prone to errors. A blockchain-based solution is poised to solve the problems by providing sharable KYC and AML data with tamper resistance and security. KYC on the blockchain only requires a single entry of data, which is then protected and securely saved in immutable

TABLE 5. PoPS compared with generic consensus.

	PoW	PoS	PoPS PoTD
Applicability	Public	Public	Consortium
Node elected on	Computing Power	Stake	Premium and Density
Decentralization	High	High	NA
Accounting nodes	Whole network	Whole network	Selected nodes
Computing Overhead	High	Medium	Low
Network Overhead	Low	Low	Least
Storage Overhead	High	High	Low
Scalability	Not scalable	Scalable	Scalable
Security	51% attack possible	less prone to 51% at- tack	NA
Mining Rewards	Mining + Transaction fee	Coin stacked + Transaction Fee	Subscription fee for stakeholders

ledgers. Insurers don't need to process the customer KYC again; they can query and verify from the immutable ledgers. The use of blockchain for financial businesses can also streamline the compliance process and reduce overhead costs and overhead time. This also eliminates the need for a manual complaint report, as regulators can access all the regulatory confirmation and audit information in real-time.

KYC process on the proposed framework would include smart contracts for fetching data and aggregating from various authentic resources on ecosystem. The data is presented as a shareable, tamper resists customer data, with secure privacy preserved cooperation among the stakeholder, reduce redundant work and save time. In addition, improves compliance and regulatory standards by providing real-time visibility of the activities on the network.

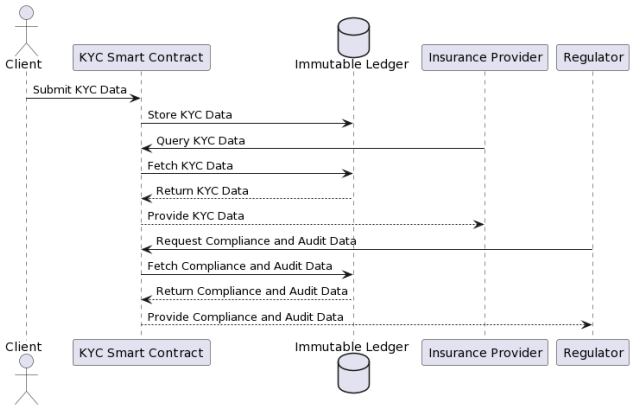


FIGURE 16. Workflow of KYC.

Fig. 16 illustrates a workflow for an insurance system involving clients, a KYC smart contract on a blockchain, an immutable ledger, an insurance provider and a regulator.

Key components of a platform-agnostic blockchain and IoT based insurance framework:

1) Clients submit KYC data to the smart contract, which stores it on the immutable ledger.
2) The smart contract enables authorized parties to query and fetch KYC data.
3) Insurance providers request compliance and audit data from the smart contract.
4) Insurance providers share compliance and audit data with regulators.

The blockchain ensures data integrity and security. Smart contracts automate data management processes. The platform-agnostic design allows implementation on various blockchain platforms. IoT devices can be integrated to automatically submit data to the smart contract, such as identity verification or asset tracking.

This framework combines blockchain and IoT to create a transparent, secure and automated insurance system, simplifying compliance and audit processes while protecting client data. The decentralized architecture enhances trust and efficiency.

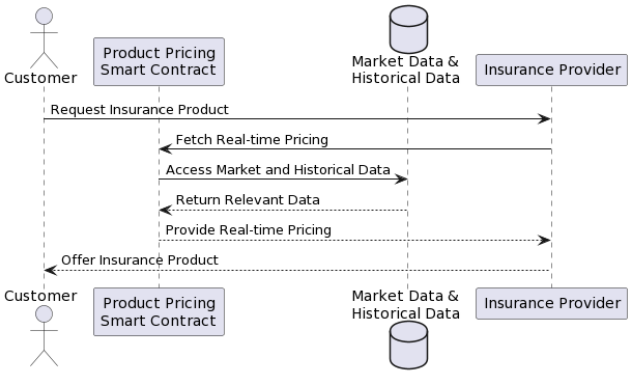


FIGURE 17. Workflow of product pricing.

B. WORKFLOW OF PRODUCT PRICING

In a conventional home product design, the actuary, domain experts, business intelligence and market analytics teams have to crunch data from contracts, policy queries, real-world data from the field and customer needs. Despite extended data and work, the product design is not dynamic; it is prone to be outdated before the actual product is sold by the intermediaries due to dynamic evolution and changes in market dynamics. Most of the product pricing is based on historical data collected by the data analytics team and there is a constant gap between the current data collected by the analytics team and the real world. This gap led to poor insurance product design and an inability to cover at a granular level. These conventional models are known to

cover as a whole and individual coverages for items are added as extra riders, but the claim process is mostly as a whole.

Insurance marketplace on the proposed framework would include smart contract for Real- time product pricing, dynamic marketplace, direct access to customers and providers and transaction are fast and autonomous.

The Fig. 17 depicts a workflow involving a Customer, Product Pricing Smart Contract, Market Data & Historical Data and an Insurance Provider, automating the insurance product pricing and offering process.

Key steps in the workflow:

1) Customer request an insurance product from the Product Pricing Smart Contract.
2) Smart Contract fetches real-time pricing by accessing market and historical data.
3) Smart Contract calculates real-time pricing using the retrieved data.
4) Smart Contract provides the real-time pricing offer to the Customer.
5) If the Customer accepts the offer, they communicate acceptance to the Smart Contract.
6) Smart Contract relays Customer's acceptance to the Insurance Provider to establish the contract.

The smart contract automates the pricing and offering process by: Integrating real-time market data and historical data for dynamic, personalized pricing, Serving as an intermediary between Customer and Insurance Provider and Handling data lookup, pricing calculations and facilitating the agreement.

Benefits of this automated workflow compared to traditional manual pricing methods: Increased efficiency and transparency, Responsiveness to market conditions and Improved customer experience through personalized, real-time pricing.

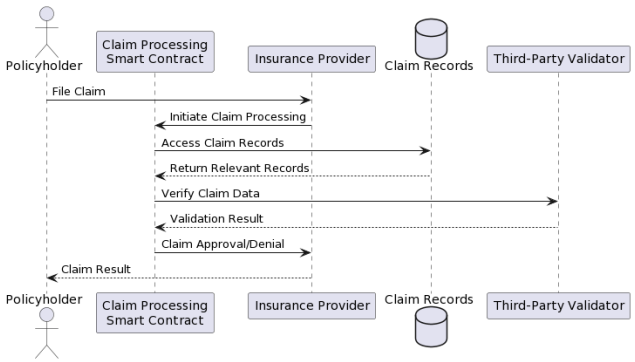


FIGURE 18. Workflow for automated claim processing.

C. WORKFLOW FOR AUTOMATED CLAIM PROCESSING

The majority of the tasks that insurance companies must complete include filing, validating and approving claims. Blockchain's trustless identity verification and smart contracts enable automatic and faster claim processes. Smart contracts can hold funds that have not yet been assigned to the policyholder or allocated to the insurance company because they act as an intermediary. The right party receives the funds when an event activates the smart contract. In the past, approving a claim took a week or a month, even though it involved numerous web portal updates, paper paperwork and photocopies. Automate information collection and processing through smart contracts and Improve data access and visibility. Lower overall cost due to faster transactions and processes automated by smart contracts

Claim handling processes on the proposed framework would include smart contracts to create a trusted environment, tamper proof and shareable claim record within the consortium, eliminating the fraudulent claim. Provide customer data privacy during data sharing silos.

The Fig. 18 illustrates the workflow of an insurance claim processing system involving a Policyholder, Claim Processing Smart Contract, Insurance Provider, Claim Records and Third-Party Validator.

Key steps in the claim processing workflow:

1) Policyholder files a claim through the Claim Processing Smart Contract.
2) Smart Contract initiates claim processing and accesses relevant claim records.
3) Smart Contract retrieves relevant records needed to process the claim.
4) Smart Contract verifies claim data for completeness, consistency and validity based on predefined rules.
5) Verified claim data is sent to the Insurance Provider.
6) Insurance Provider validates the claim, possibly involving manual review and approval.
7) Validation result is returned to the Smart Contract.
8) If the claim is approved, Smart Contract generates claim approval/denial and associated details.
9) Claim result is provided to the Policyholder.

The smart contract automates significant portions of the claim processing by: Handling initial data verification, Coordinating data flow between Policyholder, Insurance Provider and Claim Records. The Third-Party Validator adds an extra layer of validation and trust to the process.

Benefits of automating the insurance claim process with a smart contract: Increased efficiency and consistency compared to manual processing, Enhanced transparency and trustworthiness through rules-based processing and Immutable audit trail provided by blockchain-based claim records.

D. WORKFLOW FOR COUNTERING FRAUD TRANSACTION

Blockchain, with its powerful smart contracts and connected IoT, provides a remedy for fraud mitigation by enabling secure data sharing and intelligence among insurers. Blockchain, with its ideal decentralised model, immutability and privacy-protected transparency, is the current de facto standard to preserve data and prevent fraud. The technology's granular privacy control property helps to provide selective data sharing among the user and consortium. Transaction

fraud in the conventional system is mostly carried due to lags or delays in the convergence of information and a lack of intelligence and incident sharing among the insurance provider and across the stakeholder

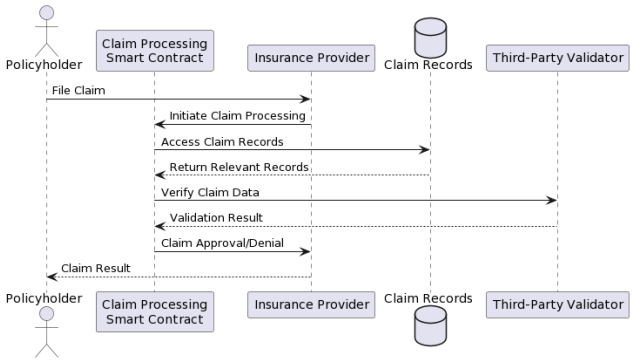


FIGURE 19. Workflow for countering fraud transaction.

The Fig. 19 depicts a workflow involving an IoT Sensor, User, Anti-Fraud Smart Contract, Insurance Provider, Transaction Records and a Fraud Detection System, integrating these components to prevent insurance fraud.

Key steps in the workflow:

1) IoT Sensor provides data to the User.
2) User initiates a transaction through the Anti-Fraud Smart Contract.
3) Smart Contract verifies the transaction, checking for signs of fraud based on predefined rules and transaction history.
4) Smart Contract accesses transaction history from the Transaction Records.
5) Relevant records are returned to the Smart Contract for analysis.
6) Analyzed transaction data is sent to the Insurance Provider.
7) Insurance Provider sends data to the Fraud Detection System for further analysis.
8) Fraud Detection System analyzes data, potentially using machine learning to identify fraud patterns.
9) Fraud Detection Result is returned to the Smart Contract.
10) Based on the fraud analysis, Smart Contract generates a Transaction Approval/Denial.
11) Transaction Result is provided to the User.

The integration of technologies in this workflow enhances the insurance process by: Using IoT sensor data to verify claims and provide real-world data, Automating initial fraud screening with the smart contract's predefined rules and transaction history and Leveraging a specialized Fraud Detection System for sophisticated analysis and AI-based pattern recognition.

Benefits of this data-driven, automated and fraud-resistant approach: Increased efficiency and accuracy in fraud detection, Reduced manual intervention and human error and Immutable transaction records on the blockchain ensure data integrity and provide an audit trail.

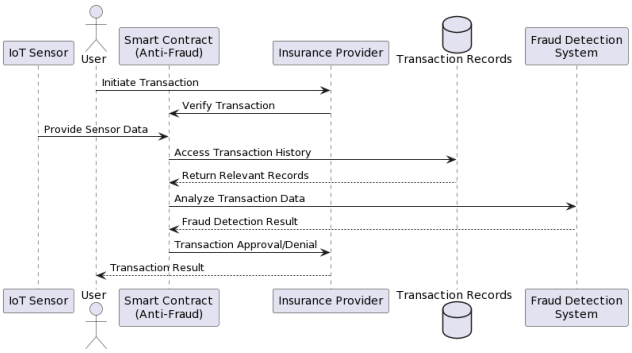


FIGURE 20. Autonomous real-time claim and payment.

E. AUTONOMOUS REAL-TIME CLAIM AND PAYMENT

Blockchain, IoT and contracts with secure and non-repudiation frameworks enable the customer to get an autonomous environment where claims are made automatically and payment is settled in real-time. The proposed novel framework is crucial of its kind and can bring a great revolution to home insurance which lacks a parametric model.

Underwriting, is an essential step that must be preceded by skilled data analysis in order to calculate a customer's coverage and define that customer's insurance coverage. The data storage, administration and analysis facilities provided by blockchain have made it possible for underwriters' work to be carried out in an effective, rapid and risk-free manner. In addition, it brings a higher degree of openness to the underwriting process, which in turn helps to increase clients' trust in insurance firms. A smart contract based implementation would help an automated underwriting process.

Data pool is the store house of all the data in the ecosystem. The storage, processing and administration of massive volumes of data that insurance firms are able to store efficiently on blockchains is the most significant use case of blockchain technology. Blockchains may be used to store this data efficiently. Additionally, it improves the manner in that various parties may exchange and access this data while also streamlining the process. Using techniques such as fingerprinting and timestamping, blockchain technology enables the creation of a repository that is both safe and accessible to all parties involved, including insurance firms and policy- holders. This enables insurance firms to work with risks that are manageable and quantified, which in turn facilitates a fantastic experience for customers and ensures trust is smoothly delivered. The analytic smart contracts depend on the data pool for data feed.

The Fig. 20 illustrates a complex workflow involving a Customer, IoT Sensor, Underwriting Smart Contract, Insurance Provider, Data Pool, Claims Records, Analytics

Smart Contract and Bank, integrating these components to automate the end-to-end insurance process.

Key steps in the workflow:

1) Customer requests coverage through the IoT Sensor.
2) IoT Sensor provides sensor data to the Underwriting Smart Contract.
3) Smart Contract assesses the coverage request using the sensor data.
4) Smart Contract retrieves relevant data from the Data Pool.
5) Retrieved data is used to define the coverage and premium.
6) Smart Contract offers an insurance policy to the Customer.

If the Customer accepts the offer:

7) Customer reports a claim, providing claim data.
8) Smart Contract validates the claim.
9) Smart Contract accesses the claim history from the Claims Records.
10) Relevant data is requested from the Analytics Smart Contract.
11) Analytics Smart Contract returns the requested data.
12) Claim validation result is determined.
13) If approved, a payment request is sent to the Bank.
14) Bank provides payment confirmation.
15) Claim payment is made to the Customer.

The integration of technologies in this workflow enhances the insurance process by: Using IoT sensor data and data pools for data-driven, personalized coverage. Automating policy offering, claim validation and payment with smart contracts and Leveraging an analytics smart contract for advanced data processing capabilities.

Benefits of this sophisticated, automated insurance workflow: Increased efficiency and accuracy across the entire insurance process, Reduced manual intervention and human error, Enhanced data integrity and audit trail through blockchain records. and Improved customer experience with personalized coverage and streamlined claims processing.

F. REINSURANCE AND REINSURANCE CLAIM HANDLING

Reinsurance is the practice of insurers purchasing additional coverage from third parties to mitigate their overall risk exposure. Blockchain technology can help automate calculations, track financial risks and enhance reinsurance policies. Reinsurance claim handling is crucial for insurers' risk management, but it often involves multiple parties with varying data standards, complicating reconciliation and information flow.

Smart contracts on the blockchain can efficiently handle multiple parties at different hierarchical levels. By providing tamper-proof, time-stamped records of claims, blockchain enables a single source of truth, eliminates manual reconciliation, standardizes reporting and enhances risk management. Smart contracts can also automate reinsurance accounting, streamlining cash flows.

Peer-to-peer (P2P) insurance involves individuals pooling resources to insure each other against risks. Blockchain can provide the trust needed for a self-sufficient P2P transaction network. Smart contracts can partially automate claim payouts by checking documentation and claim amounts. P2P groups can also use secure voting mechanisms on the blockchain to approve or refuse claims, simplifying payouts. Some P2P groups may purchase reinsurance for extra protection, with reinsurers using smart contracts to enforce specific terms before claim payouts are made.

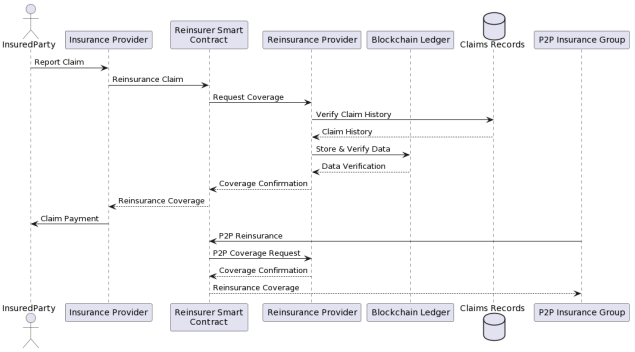


FIGURE 21. Reinsurance and reinsurance claim handling.

The Fig. 21 illustrates a workflow for an insurance system that integrates IoT and blockchain technologies. The key components are:

1) InsuredPart, Reports claims and is part of a P2P insurance group.
2) Insurance Provider, Manages claims, requests reinsurance and pays claims.
3) Reinsurer Smart Contract, Facilitates reinsurance transactions on the blockchain.
4) Reinsurance Provider, Provides reinsurance coverage to the Insurance Provider.
5) Blockchain Ledger, Immutably stores claims records and reinsurance transactions.
6) Claims Records, Database for storing and verifying claim data.

IoT devices collect data from the InsuredParty, while the blockchain secures reinsurance transactions and maintains an immutable ledger. The smart contract automates reinsurance logic, enabling a platform-agnostic, decentralized insurance marketplace. This framework combines IoT for data collection and blockchain for reinsurance contracts and record-keeping, creating an automated, secure and efficient insurance system.

All of the proposals in the proposed framework when implemented in real-time, would provide a better customer experience and prevent losses incurred by insurance companies.

VII. CONCLUSION

The adaptation of nascent technology has a few limitations and adopting blockchain for insurance is no exception to

the limitations. The technology is quite evolving and is still resolving issues like transaction speed optimization, convergence challenges, data security and verification models. Large enterprise systems have strict regulatory practices and compliance needs. Financial domains need to meet critical and complex regulations.

In its evolving stage, blockchain faces difficulties with quick adoption and frequent regulatory updates in the financial domain. While robust security and privacy are much talked about in blockchain, the design decision on the use of this type of technology has many adopters concerned. The constant need for upgrades in security and privacy is a continuous process for enterprise adopters. The integration challenge brings limitations to bridging legacy systems to the blockchain ecosystem; either a significant trade-off to adopt a new system feature or an overhaul of the existing system is required. Operation time in the ever-changing blockchain implementation is not yet mature enough due to hardware and software related changes to comment on the optimal performance time. With this said, the customer's needs and demands are always high and operational time is short. Adoption and relearning away from conventional methods are processes.

The ultimate decentralised nature of the system brings certain trade-offs and entails more conventional ways of handling data. Though the operational cost is significantly reduced by the nature of the new process redesign and the system's accessibility at a granular level, the high initial cost is a serious burden for the employers and the customers. Competition in the blockchain not only benefits multiple products but also brings in hard decision-making for the adopter and leads to misinformed customer trust and increased adoption costs. Standardization and regulation are quite difficult, given the speed at which technology is shifting gears.

Solving these limitations can provide the opportunity for early adopters to model systems around the blockchain ecosystem. Blockchain in insurance is a game changer and there are incredible benefits, cost benefits and risk reductions when you leverage blockchain. However, the technology can bring wonder if the implementation is planned with contingencies to change and adapt to the frequent updates. The use case presented is an operational framework on how Insurance domain applications can be built and operated using heterogeneous IoT nodes on multiple platform blockchains.

REFERENCES

[1] S. Azeez Syed, V. Sinha, S. Singh, and A. Goel, "Blockchain framework for data storage and security," in *Recent Advances in IoT and Blockchain Technology*, 2022, pp. 1–43.

[2] S. Krishnamurthy, S. V. Mony, N. Jhaveri, S. Bakhshi, R. Bhat, M. R. Dixit, S. Maheshwari, and R. Bhat, "Insurance industry in India: Structure, performance, and future challenges," *Vikalpa, J. Decis. Makers*, vol. 30, no. 3, pp. 93–120, Jul. 2005.

[3] T. Alladi, V. Chamola, R. M. Parizi, and K. R. Choo, "Blockchain applications for industry 4.0 and industrial IoT: A review," *IEEE Access*, vol. 7, pp. 176935–176951, 2019.

[4] P. K. Meduri, S. Mehta, K. Joshi, and S. Rane, "Disrupting insurance industry using blockchain," in *Proc. Int. Conf. Intell. Data Commun. Technol. Internet Things (ICICI)*. Cham, Switzerland: Springer, 2018, pp. 1068–1075.

[5] R. Brophy, "Blockchain and insurance: A review for operations and regulation," *J. Financial Regulation Compliance*, vol. 28, no. 2, pp. 215–234, May 2020.

[6] S. Kumar, U. Dohare, and O. Kaiwartya, "FLAME: Trusted fire brigade service and insurance claim system using blockchain for enterprises," *IEEE Trans. Ind. Informat.*, 2022.

[7] A. K. Kar and L. Navin, "Diffusion of blockchain in insurance industry: An analysis through the review of academic and trade literature," *Telematics Informat.*, vol. 58, May 2021, Art. no. 101532.

[8] E. Chondrogiannis, V. Andronikou, E. Karanastasis, A. Litke, and T. Varvarigou, "Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health insurance organizations," *Blockchain, Res. Appl.*, vol. 3, no. 2, Jun. 2022, Art. no. 100049.

[9] S. Goyal, S. K. Sharma, and P. K. Bhatia, "Blockchain for the security and privacy of IoT-based smart homes," in *Blockchain Technology for Data Privacy Management* (Advances in intelligent decision-making, systems engineering, and project management). Boca Raton, FL, USA: CRC Press, 2021, pp. 239–252.

[10] S. Sun, R. Du, S. Chen, and W. Li, "Blockchain-based IoT access control system: Towards security, lightweight, and cross-domain," *IEEE Access*, vol. 9, pp. 36868–36878, 2021.

[11] S. Trivedi and R. Malik, "Blockchain technology as an emerging technology in the insurance market," in *Big Data: A Game Changer for Insurance Industry*, 2022, pp. 81–100.

[12] S. Cousaert, N. Vadgama, and J. Xu, "Token-based insurance solutions on blockchain," in *Blockchains and the Token Economy*. Cham, Switzerland: Springer, 2022, pp. 237–260.

[13] S. Grima, J. Spiteri, and I. Romānova, "A STEEP framework analysis of the key factors impacting the use of blockchain technology in the insurance industry," *Geneva Papers Risk Insurance-Issues Pract.*, vol. 45, no. 3, pp. 398–425, Jul. 2020.

[14] L. B. Krithika, "Survey on the applications of blockchain in agriculture," *Agriculture*, vol. 12, no. 9, p. 1333, Aug. 2022.

[15] O. Johnson, "Decentralized reinsurance: Funding blockchain-based parametric bushfire insurance," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2022, pp. 1–3.

[16] L. Ismail and S. Zeadally, "Healthcare insurance frauds: Taxonomy and blockchain-based detection framework (Block-HI)," *IT Prof.*, vol. 23, no. 4, pp. 36–43, Jul. 2021.

[17] A. A. Amponsah, A. F. Adekoya, and B. A. Weyori, "A novel fraud detection and prevention method for healthcare claim processing using machine learning and blockchain technology," *Decis. Anal. J.*, vol. 4, Sep. 2022, Art. no. 100122.

[18] M. Kherbouche, G. Pisoni, and B. Molnár, "Model to program and blockchain approaches for business processes and workflows in finance," *Appl. Syst. Innov.*, vol. 5, no. 1, p. 10, Jan. 2022.

[19] T. Dominguez Anguiano and L. Parte, "The state of art, opportunities and challenges of blockchain in the insurance industry: A systematic literature review," *Manage. Rev. Quart.*, vol. 74, no. 2, pp. 1097–1118, Jun. 2024.

[20] A. A. Amponsah, A. F. Adekoya, and B. A. Weyori, "Improving the financial security of national health insurance using cloud-based blockchain technology application," *Int. J. Inf. Manage. Data Insights*, vol. 2, no. 1, Apr. 2022, Art. no. 100081.

[21] N. Sharma and R. Rohilla, "Blockchain based electronic health record management system for data integrity," in *Proc. Int. Conf. Comput. Intell.* Springer, 2022, pp. 289–297.

[22] D. Wilusz and A. Wójtowicz, "Secure protocols for smart contract based insurance services," *Expert Syst.*, vol. 39, no. 9, Nov. 2022, Art. no. e12950.

[23] I. Tibrewal, M. Srivastava, and A. K. Tyagi, "Blockchain technology for securing cyber-infrastructure and Internet of Things networks," in *Intelligent Interactive Multimedia Systems for E-Healthcare Applications*. Cham, Switzerland: Springer, 2022, pp. 337–350.

[24] R. Khatwani, M. Mishra, M. Bedarkar, K. Nair, and J. Mistry, "Impact of blockchain on financial technology innovation in the banking, financial services and insurance (BFSI) sector," *J. Statist. Appl. Probab.*, vol. 12, no. 1, pp. 181–189, 2023.

[25] A. Sidiqqui and K. J. Tansen, "Blockchain: A disruptive technology," in *Blockchain Technology and Computational Excellence for Society 5.0*. IGI Global, 2022, pp. 48–58.
[26] A. Shetty, A. D. Shetty, R. Y. Pai, R. R. Rao, R. Bhandary, J. Shetty, S. Nayak, T. K. Dinesh, and K. J. Dsouza, "Block chain application in insurance services: A systematic review of the evidence," *SAGE Open*, vol. 12, no. 1, Jan. 2022, Art. no. 215824402210798.
[27] H. Albrecher, D. Finger, and P.-O. Goffard, "Blockchain mining in pools: Analyzing the trade-off between profitability and ruin," *Insurance, Math. Econ.*, vol. 105, pp. 313–335, Jul. 2022.
[28] H. Zheng, L. You, and G. Hu, "A novel insurance claim blockchain scheme based on zero-knowledge proof technology," *Comput. Commun.*, vol. 195, pp. 207–216, Nov. 2022.
[29] E. Sutanto, R. Mulyana, F. C. S. Arisgraha, and G. Escrivá-Escrivá, "Integrating blockchain for health insurance in Indonesia with hash authentication," *J. Theor. Appl. Electron. Commerce Res.*, vol. 17, no. 4, pp. 1602–1615, Nov. 2022.
[30] A. Karmakar, P. Ghosh, P. S. Banerjee, and D. De, "ChainSure: Agent free insurance system using blockchain for healthcare 4.0," *Intell. Syst. Appl.*, vol. 17, Feb. 2023, Art. no. 200177.
[31] P. Gangwani, T. Bhardwaj, A. Perez-Pons, H. Upadhyay, and L. Lagos, "On the convergence of blockchain and IoT for enhanced security," in *Artificial Intelligence in Cyber-Physical Systems*. Boca Raton, FL, USA: CRC Press, 2023, pp. 35–49.
[32] P. Gangwani, S. Joshi, H. Upadhyay, and L. Lagos, "IoT device identity management and blockchain for security and data integrity," *Int. J. Comput. Appl.*, vol. 184, no. 42, pp. 49–55, Jan. 2023.
[33] G. Jayabalasamy and S. Koppu, "High-performance Edwards curve aggregate signature (HECAS) for nonrepudiation in IoT-based applications built on the blockchain ecosystem," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 10, pp. 9677–9687, Nov. 2022.

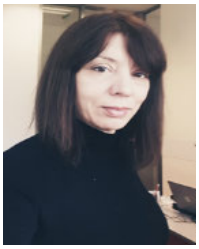
J. GURUPRAKASH received the Ph.D. degree from the Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Coimbatore, India. He is a Faculty Member with the Amrita Vishwa Vidyapeetham. With over 15 years of experience in both the IT industry and academia, he has developed a wealth of knowledge and expertise in his field with research interests focused on exploring cutting-edge technologies, including blockchain technologies, the Internet of Things (IoT), and artificial intelligence/machine learning (AI/ML).

DIMITAR TOKMAKOV received the Ph.D. degree in electronics engineering from the Technical University of Sofia, Sofia, Bulgaria, in 2011. He is a Professor of communication and computer engineering with the University of Plovdiv Paisii Hilendarski, Plovdiv, Bulgaria. His research interests include e-learning, artificial intelligence, wireless communications, the Internet of Things, and computer communications.

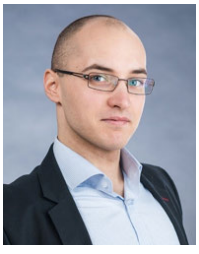
L. B. KRITHIKA received the Ph.D. degree in image processing from Vellore Institute of Technology (VIT), India. Currently, she is an Senior Assistant Professor with more the 14 years of collective experience as an innovative result oriented Teacher with SCORE, VIT. She was also a Committed Trainer of the Cisco Net Academy, in 2010; and VIT. She has published more than 20 international/national journals and conferences with high impact factor journals. Her research interests include image processing, machine learning, the Internet of Things, and blockchain.

SRINIVAS KOPPU received the Ph.D. degree from Vellore Institute of Technology (VIT), India. He has more than 14 years of experience in teaching. He was a Visiting Professor with the Neusoft Institute of Information Technology, China, in 2018. He is currently an Associate Professor (Senior) with the SCORE, VIT. He is a Co-Principal Investigator of the British Council Grant Industry-Academia Collaborative Grant (2022–2023) of the Project "Co-Designing a Smart Curriculum and Personalized Method of Delivery for Inclusive Value Added Courses," which was received from the University of Nottingham, U.K. He has published more than 30 international/national journals and conferences. His research interests include deep learning, federated learning, blockchain technologies, the IoT, data analytics, cryptography, medical image processing, image security analysis, video processing, computer vision, and high-performance computing.

R. SRINIVASA PERUMAL received the Ph.D. degree from Vellore Institute of Technology, Vellore. He is currently an Associate Professor (Senior) with the School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India. He has published several refereed research papers in various international journals and conferences. His current research interests include digital image processing, pattern recognition, computer vision, multimodal biometrics, medical imaging, software engineering, and the IoT.



ANNA BEKYAROVA-TOKMAKOVA is currently pursuing the Ph.D. degree with the University of Plovdiv Paisii Hilendarski, Plovdiv, Bulgaria. She is also an Assistant Professor with the University of Plovdiv Paisii Hilendarski. Her research interests include artificial intelligence, management, telecommunications, and the Internet of Things.



MIHAIL MILEV received the degree in electronics and information and communication technologies. He is currently pursuing the Ph.D. degree with the University of Plovdiv Paisii Hilendarski, Plovdiv, Bulgaria. During his carrier in the automotive industry, he specialized in embedded systems security. He researches various topics on cyber security.