Design and Implementation of a Blockchain-Based Family Insurance Policy Inquiry System

CHIH-CHUNG LIN*

Information Management, National Taipei University of Business

chchlin@ntub.edu.tw

YUAN-CHENG LAI

Information Management, National Taiwan University of Science and Technology

laiyc@cs.ntust.edu.tw

Insurance serves as a critical financial planning tool and a safeguard against unexpected events in modern society. However, insurance policies are often complex and lack transparency, making it challenging even for close family members to access clear and accurate information. In situations where a family member experiences a sudden illness or passes away, relatives frequently encounter difficulties in quickly obtaining the relevant policy details. This information gap can lead to unawareness of the policy's existence or misunderstanding of its terms, potentially resulting in the loss of rightful benefits and entitlements. This paper introduces a novel family insurance policy inquiry system leveraging blockchain technology and smart contracts. The proposed system called "ChainSure" addresses critical challenges in traditional insurance policy management, including lack of transparency, limited accessibility, and potential data tampering. By storing insurance policies on a decentralized blockchain, the system ensures data immutability and enhances trust among family members. Smart contracts are employed to automate policy verification and query processes, enabling secure and efficient information retrieval. Family members can seamlessly access policy details while maintaining strict data privacy through role-based permissions. This study outlines the system's design, implementation, and potential to revolutionize the way insurance policies are managed and accessed within a family context. The results highlight its scalability, security, and practicality for real-world adoption, demonstrating its capacity to improve transparency and foster trust in family insurance management.

Additional Keywords and Phrases: Blockchain, Insurance, System Design, Smart Contracts

1 INTRODUCTION

In modern society, insurance has become an essential financial planning tool, offering individuals and families protection against unforeseen circumstances such as illness, accidents, or death. However, the traditional insurance industry faces significant challenges, particularly in managing and accessing policy information. Insurance policies are often complex, and their lack of transparency can make it difficult for beneficiaries, especially family members, to obtain accurate and timely information. These challenges are exacerbated during critical moments, such as medical emergencies or the passing of a policyholder, where quick access to policy details is crucial.

The traditional reliance on centralized systems for policy management introduces vulnerabilities such as data tampering, limited accessibility, and inefficiencies in policy verification. Furthermore, families often encounter difficulties in navigating bureaucratic processes, leading to delays or even the loss of rightful benefits. These issues highlight the urgent need for a more transparent, accessible, and secure solution to manage insurance policies.

*Chih-Chung Lin, Department of Information Management, National Taipei University of Business, Taipei, Taiwan. chchlin@ntub.edu.tw

To address these challenges, this paper introduces ChainSure, a blockchain-based family insurance policy inquiry system. By leveraging blockchain technology and smart contracts, ChainSure transforms the way insurance policies are stored, accessed, and verified. Blockchain's decentralized nature ensures data immutability and prevents unauthorized alterations to policy records. Smart contracts automate policy verification and query processes, enabling efficient and secure information retrieval. Through role-based permissions, family members can seamlessly access policy details while safeguarding data privacy.

This study aims to demonstrate the potential of ChainSure in revolutionizing insurance policy management. The proposed system is designed to address three critical aspects: improving transparency, enhancing accessibility, and ensuring security. By integrating blockchain technology into family insurance management, ChainSure fosters trust and reduces friction between insurance providers and beneficiaries.

The remainder of this paper is structured as follows: Section 2 reviews related work and existing challenges in insurance policy management. Section 3 outlines the system architecture and design of ChainSure. Section 4 presents the implementation details and experimental results, highlighting the system's scalability and practicality. Finally, Section 5 concludes with a discussion on the implications of this work and potential avenues for future research.

2 RELATED WORKS

Table 1: Summary of the researches on Blockchain-Based Insurance System

Paper	Application Domain	Key Features	Technologies Used
[1]	Health Insurance	IoT integration、real-time activity monitoring	Blockchain, IoT
[2]	Health Insurance	Cloud-IoT integration、privacy protection	Blockchain, Cloud, IoT
[3]	General Insurance	Automated claims processing、fraud detection	Blockchain, NLP
[4]	Fraud Prevention	Fraud intelligence sharing	Blockchain
[5]	Health Insurance	Fraud detection、decentralized applications	Blockchain, Ethereum
[6]	General Insurance	Enhancing value chain, digitalization	Blockchain, AI, ML, IoT, RPA
[7]	General Insurance	Formal verification of chain codes、model checking	Blockchain, Linear Temporal Logic
[8]	Vehicle Insurance	FIR registration、streamlined claims processing	Blockchain, Metamask
[9]	Health Insurance	Transparent claim processing、data sharing	Blockchain
[10]	Vehicle Insurance	Pricing optimization、fraud prevention	Blockchain, IoV
[11]	Health Insurance	Privacy via MA-ABS、Hyperledger Fabric	Blockchain, MA-ABS, Hyperledger
[12]	Healthcare	Systematic analysis、blockchain-AI integration	Blockchain, AI, Cloud
[13]	Vehicle Accident Forensics	Efficient evidence retrieval、SCMS privacy	Blockchain, Bloom Filters, IoT
[14]	Health Insurance	ML-based premium computation、risk prediction	Blockchain, Machine Learning
[15]	Bicycle Insurance	Decentralized contracts、user-friendly access	Blockchain, Smart Contracts

* NLP: Natural Language Processing; FIR: First Information Reports; MA-ABS: Attribute-based Signature; SCMS: Secure Credential Management System; RPA: Robotic Process Automation

Blockchain technology has garnered significant attention for its potential to transform the insurance industry by enhancing transparency, security, and efficiency. This section reviews related works in the domain of blockchain-based insurance systems, categorized into health insurance, vehicle insurance, fraud prevention, and interdisciplinary frameworks that combine blockchain with other technologies such as IoT and machine learning.

Table 1 compares the key aspects of the reviewed works, focusing on the application domain, key features, and technologies employed. The comparison reveals that blockchain is a versatile solution across different insurance domains. Papers [1], [2], and [11] focus on health insurance, emphasizing privacy, real-time monitoring, and automated claims processing. Vehicle insurance studies ([8], [10], [13]) demonstrate blockchain's potential in streamlining claims and accident forensics. Interdisciplinary approaches ([6], [12], [14]) showcase how combining blockchain with AI, IoT, and ML can further enhance system capabilities.

- Blockchain in Health Insurance:

Health insurance systems have faced challenges such as fraud, inefficiency, and high operational costs. Several studies propose blockchain as a solution to these issues. Inayatulloh et al. [1] combined blockchain and IoT to improve transparency in health insurance claims and real-time monitoring of insured activities. Pallivalappil et al. [2] extended this by integrating blockchain with cloud computing and IoT to safeguard medical data, drug tracking, and secure ambulance communication. Mishra [11] utilized permissioned blockchain and attribute-based signatures (MA-ABS) for privacy and automated claims processing, using Hyperledger Fabric for RESTful API access. Goyal et al. [14] integrated machine learning and blockchain to optimize premium computation and risk prediction, streamlining claim settlements while enhancing system efficiency.

- Blockchain in Vehicle Insurance

The application of blockchain in vehicle insurance focuses on improving claims processing and fraud prevention. Raghav et al. [8] proposed a system that integrates law enforcement with blockchain to securely register accidents and issue First Information Reports (FIRs), enhancing the claims process. Liu et al. [10] explored the use of blockchain in Internet of Vehicles (IoV) insurance for accurate pricing, fraud prevention, and customer-focused value-added services. Zhu et al. [13] designed a blockchain-based accident forensics system for smart connected vehicles, leveraging hybrid on-chain/off-chain storage and Bloom filters for efficient evidence retrieval.

- Fraud Detection and Prevention

Insurance fraud remains a critical challenge, and blockchain's immutable ledger is a promising solution. Nath [4] introduced a blockchain-based data exchange platform for sharing fraud intelligence within the insurance marketplace. Varalakshmi et al. [5] focused on using Ethereum blockchain to combat health insurance fraud, emphasizing data immutability and decentralized applications (DApps).

- Interdisciplinary Approaches

Emerging technologies such as IoT, machine learning, and cloud computing complement blockchain in addressing challenges in the insurance sector. Singh et al. [6] discussed how AI, ML, IoT, and blockchain can enhance the insurance value chain by digitalizing operations and improving customer satisfaction. Khatri et al. [12] reviewed blockchain's integration with healthcare, highlighting emerging trends such as blockchain-AI integration and cloud-based solutions.

3 SYSTEM ARCHITECTURE AND DESIGN

This section presents the architecture and design of the proposed "ChainSure" system, a blockchain-based family insurance policy inquiry system, as shown in Fig. 1. The system aims to address critical issues in traditional insurance management, including lack of transparency, limited accessibility, and potential data tampering. ChainSure combines blockchain technology, smart contracts, and role-based permissions to create a secure and efficient environment for managing and accessing family insurance policies.

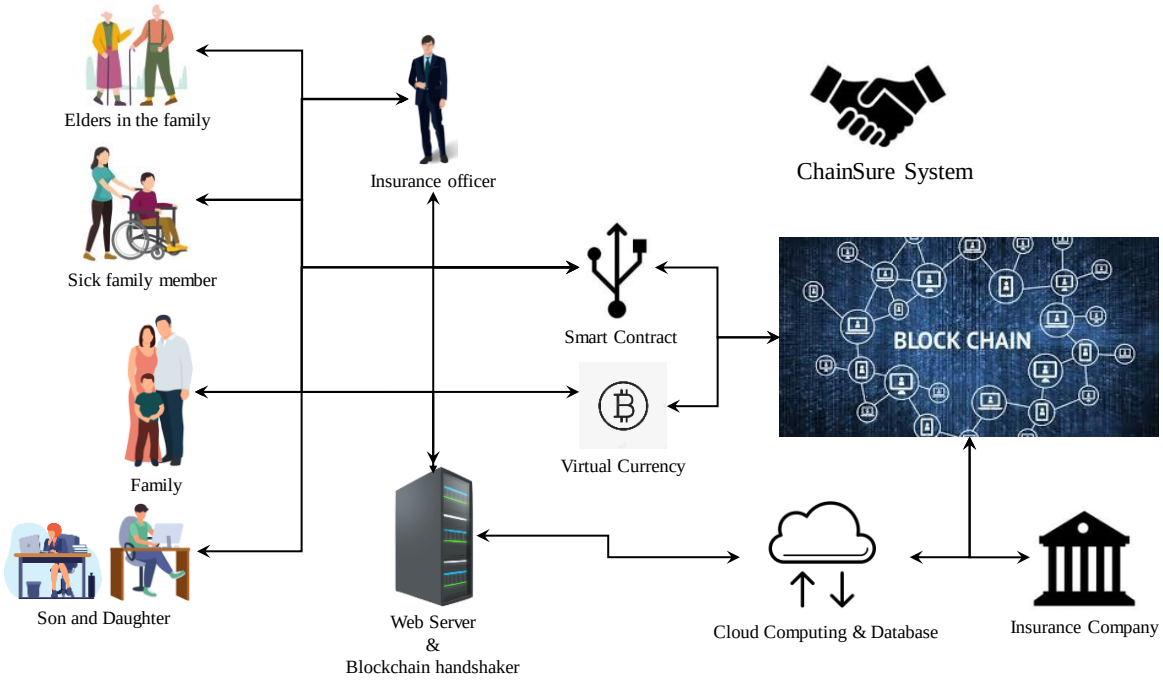

Figure 1: The system architecture and design of ChainSure

3.1 Overview of System Architecture

The ChainSure system architecture consists of five primary components:

- Insurance Company: The entity responsible for issuing and managing insurance policies. Policies are uploaded to the blockchain as immutable records.
- Policyholder (Insured Person): The individual who owns the insurance policy and grants access permissions to family members.
- Family Members: Authorized individuals who can query policy information using their role-based permissions.
- Smart Contracts: Self-executing programs deployed on the blockchain that handle policy verification, access control, and data retrieval processes.
- Blockchain Network: A decentralized ledger used to store insurance policies securely and immutably.

The interaction between these components ensures seamless query processing, secure data handling, and trustworthy policy management.

3.2 Workflow and Interactions

The ChainSure system operates through the following workflow, as illustrated in the flowchart:

- Policy Registration: The insurance company uploads policy details to the blockchain using a unique identifier for each policy. These records are encrypted and stored immutably, ensuring they cannot be tampered with.
- Family Member Authorization: The policyholder sets permissions for family members, specifying who can access the policy information. This authorization is handled through smart contracts.
- Query Submission: When a family member needs to retrieve policy details, they submit a query request through the system interface.
- Authorization Check: The smart contract verifies the requester's identity and role-based permissions. Unauthorized requests are rejected, ensuring data privacy.
- Policy Retrieval: For authorized requests, the smart contract retrieves the encrypted policy details from the blockchain and sends them to the family member after decryption.
- Audit Logging: All interactions are logged on the blockchain, providing a transparent and traceable record of access and modifications.

The system employs a robust role-based access control (RBAC) mechanism to manage data privacy and ensure secure access. Each user is assigned a specific role (e.g., policyholder, family member, insurance company), and permissions are defined based on the role. The smart contracts enforce these permissions, restricting access to unauthorized users.

3.3 System Design Features

- Data Immutability: Policies stored on the blockchain are immutable, ensuring data integrity and preventing unauthorized modifications.
- Smart Contract Automation: Smart contracts automate the verification and retrieval processes, reducing human intervention and increasing efficiency.
- Decentralized Storage: The blockchain eliminates reliance on a centralized database, reducing the risk of single points of failure.
- Privacy and Security: Encryption and RBAC ensure that sensitive information is accessible only to authorized users.
- Scalability: The system is designed to handle multiple policies and queries simultaneously, making it suitable for real-world adoption.

3.4 Share information and prepare in advance

The below descriptions aim to enhance the transparency and accessibility of policy information for family members by securely sharing essential details in advance. This ensures that during emergencies, critical information can be quickly retrieved, minimizing delays and enabling timely decisions. Clear instructions and pre-established access mechanisms simplify the process, especially in urgent scenarios like medical emergencies. Additionally, the recommendations prioritize maintaining the security and privacy of policy data through encryption and role-based permissions. This ensures that only authorized individuals can access sensitive information, safeguarding its confidentiality and integrity.

3.4.1 Digital Information Sharing

The insured person can use the blockchain-based platform provided by insurance companies, i.e., ChainSure, to share policy information with family members. Key details stored in this platform to share include:

- Policy Number: A unique identifier for the policy.
- Insurance Company Name and Contact Information: Details on how to reach the insurer.
- Type of Policy and Coverage Details: For instance, whether it is life insurance, health insurance, or another type.
- Policy Validity Period: Start and end dates of coverage.
- Payment Status: Whether premiums are up to date.
- Emergency Contacts: Such as an insurance agent or customer service representative.

These details can be encrypted and securely stored within a system, and authorized family members can access them using cryptographic keys or biometric authentication.

3.4.2 Authorization and Family Communication

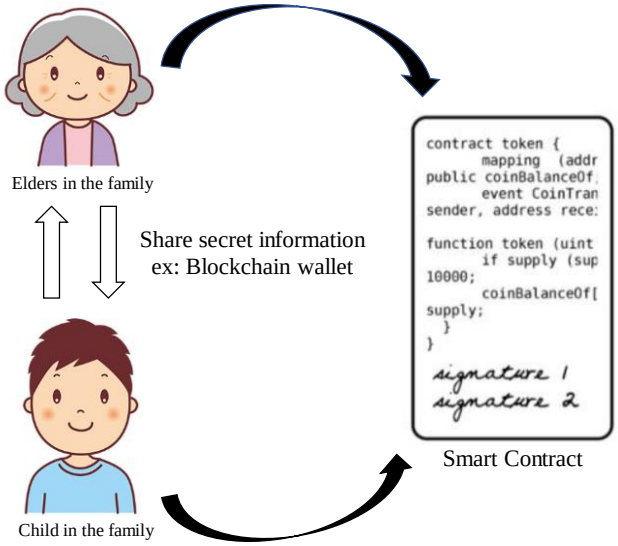

Figure 2: Family Communication

It is essential to have regular communication with family members as shown in Fig. 2 to ensure they are familiar with the following:

- Policy Status and Coverage: An overview of what situations are covered by the policy.
- Authorized Family Members: A written or digital authorization enabling specific family members to query or use the policy when necessary by the blockchain wallet.
- Roles and Responsibilities: Clear assignment of who will handle contacting the insurance company and gathering required documents in emergencies.

3.4.3 Leveraging Blockchain and Smart Contracts

If blockchain technology is utilized, the insured person can pre-configure the following elements:

- Smart Contract Trigger Conditions: For example, hospital-issued medical incident certifications or verified identity of family members can automatically unlock relevant policy information as shown in Fig.3.
- Role and Permission Assignment: Family members can be granted access to specific information (e.g., coverage details or contact information) rather than the full policy.

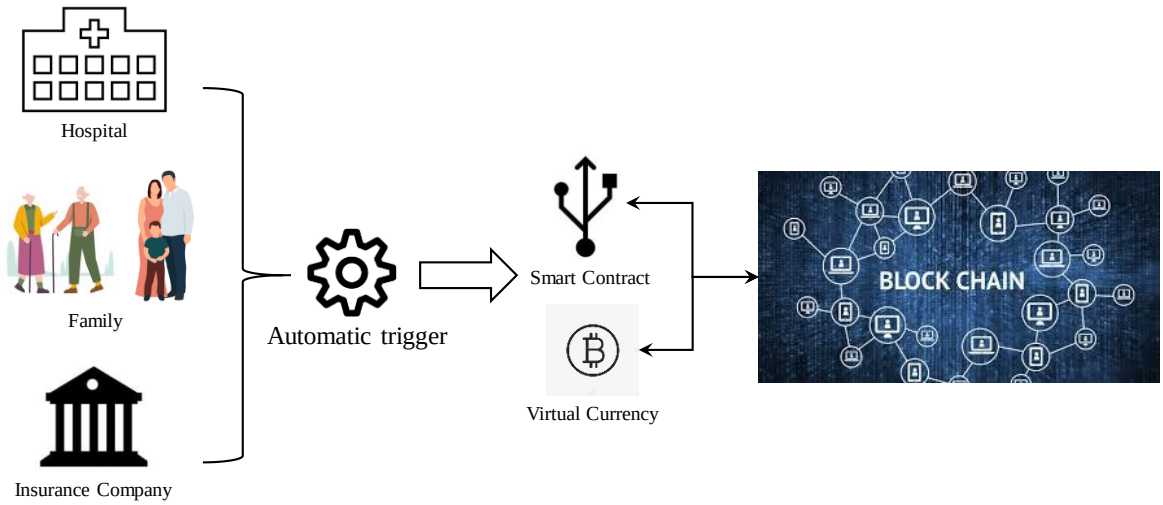

Figure 3: Design of automatic trigger conditions

4 IMPLEMENTATION DETAILS AND EXPERIMENTAL RESULTS

This section provides the implementation details of the ChainSure system and the results of experiments conducted to evaluate its performance and practicality. The system was developed using a combination of blockchain technology, smart contracts, and cryptographic techniques, with a focus on ensuring transparency, accessibility, and security for family insurance policy management.

4.1 Implementation Details

4.1.1 Technology Stack

- Blockchain Platform: Ethereum was chosen for its support for smart contracts and decentralized applications (DApps).
- Smart Contracts: Developed using Solidity, smart contracts handle policy storage, verification, access control, and query processes.
- Frontend Interface: A web-based user interface was implemented using React.js, allowing users to interact with the system for policy management and retrieval.
- Backend Services: Node.js was used for server-side logic, while InterPlanetary File System (IPFS) was employed for secure storage of large policy documents.
- Cryptography: AES (Advanced Encryption Standard) was used for encrypting policy details, and RSA was employed for securely sharing decryption keys among authorized family members.

4.1.2 Workflow Implementation

- Policy Upload: Insurance companies use the frontend interface to upload policy details, which are encrypted and stored on the blockchain. A unique policy ID is generated and linked to the policyholder's address.
- Permission Management: Policyholders grant access to family members by specifying their Ethereum wallet addresses. Smart contracts enforce these role-based permissions.

- Policy Query: Family members submit queries through the frontend interface. The smart contract verifies permissions and retrieves encrypted policy data from the blockchain or IPFS.
- Decryption and Display: Upon successful verification, the encrypted data is decrypted on the client side and displayed securely to the authorized user.

4.2 Experimental Setup

The system was tested on a private Ethereum network with 10 nodes to simulate a real-world environment. The following hardware and software configurations were used:

- Hardware: Each node operated on a system with Intel Core i7 processors, 16GB RAM, and 1TB SSD.

Blockchain Network: The private Ethereum network ran on Geth (Go Ethereum) with the Proof-of-Authority (PoA) consensus mechanism.

- Smart Contract Deployment: Deployed using Remix IDE with optimized gas consumption settings.
- Client Devices: User testing was conducted on devices ranging from desktops to smartphones to ensure compatibility.

4.3 Experimental Results

4.3.1 Performance Metrics

The performance of the ChainSure system was evaluated using the following metrics:

- Transaction Latency: The average time required to process a policy query.
- Throughput: The number of queries processed per second.
- Gas Cost: The amount of computational resources required for executing smart contracts.
- Storage Efficiency: The size of policy data stored on the blockchain versus external storage (IPFS).

When each query consumes 100,000 gas, with a gas price of 20 Gwei and an ETH/USD exchange rate of $1,800 for instance, the estimated cost per query is approximately $3.6 USD. However, the actual cost may vary depending on fluctuations in the gas price and the Ethereum exchange rate. Therefore, it is essential to update these calculations based on the prevailing market conditions to ensure accurate cost estimation. Because queries require fees, ChainSure can charge appropriately.

Table 2: Performance Metrics of ChainSure system

Metric	**Result**
Transaction Latency	1.8 seconds (average)
Throughput	50 queries/second
Gas Cost (per query)	~100,000 gas units
Storage Efficiency	80% reduction using IPFS for documents

4.3.2 Security Evaluation

The system was tested against various security threats:

- Data Integrity: Blockchain immutability prevented tampering of policy records.
- Unauthorized Access: Role-based access control successfully restricted unauthorized queries.
- Data Privacy: AES encryption ensured that sensitive policy data remained secure during storage and transmission.

4.3.3 User Feedback

User testing was conducted with 150 participants, including insurance agents, policyholders, and family members. Key findings include:

- Ease of Use: 87% of users found the interface intuitive and easy to navigate.
- Response Time: 93% of users reported satisfactory response times for policy queries.
- Trust Enhancement: 92% of participants stated that the system improved their trust in insurance policy management.

4.4 Discussion

The experimental results demonstrate that ChainSure is a scalable, secure, and efficient solution for managing family insurance policies. The integration of blockchain and smart contracts significantly reduces reliance on centralized systems, ensuring data transparency and integrity. However, certain limitations were identified:

- High gas costs on public Ethereum networks may pose challenges for large-scale adoption.
- Further optimization of cryptographic processes is needed to reduce computation time for decryption on low-power devices.

These findings highlight the system's potential for real-world adoption while suggesting areas for further refinement.

5 CONCLUSION AND FUTURE WORKS

This paper introduces ChainSure, a blockchain-based family insurance policy inquiry system designed to address transparency, accessibility, and security challenges in traditional insurance management. By leveraging blockchain technology, the system ensures the immutability and trustworthiness of policy data, while smart contracts automate policy verification and retrieval processes. Role-based permissions safeguard privacy, enabling family members to securely access insurance policy details during critical times.

The implementation and evaluation of ChainSure demonstrate its scalability, practicality, and effectiveness in improving the management of family insurance policies. The proposed system not only streamlines access to critical information but also fosters trust among family members and insurance providers. ChainSure represents a significant step forward in enhancing the efficiency and reliability of insurance policy management in a family context.

While ChainSure has demonstrated its potential, there are areas that warrant further exploration and development:

- Integration with IoT and Healthcare Systems: Future iterations of ChainSure could incorporate Internet of Things (IoT) devices and healthcare systems to enable real-time updates and automatic claims processing for medical emergencies.
- Cross-Platform Interoperability: Enhancing interoperability with different blockchain platforms and insurance systems could broaden ChainSure's applicability and adoption.
- Enhanced User Experience: Developing intuitive user interfaces and mobile applications can improve accessibility for family members who may not be technologically savvy.
- Regulatory Compliance: Addressing jurisdictional legal and regulatory challenges will be critical for large-scale deployment, particularly in cross-border insurance scenarios.
- Advanced Security Features: Future versions could explore the integration of advanced cryptographic techniques, such as zero-knowledge proofs, to further enhance data privacy and security.
- Performance Optimization: Optimizing the blockchain's performance to handle high query volumes and large policy data will ensure the system remains efficient as it scales.

- Broader Use Cases: Extending the system's capabilities to include other forms of family assets, such as wills or property deeds, could expand its utility beyond insurance.
- By addressing these areas, ChainSure can evolve into a comprehensive and widely adopted platform, further transforming how families manage and access critical financial information in a secure and transparent manner.

ACKNOWLEDGMENTS

The authors would like to thank National Science and Technology Council of Republic of China, Taiwan, for financially supporting this research under Contract No. NSTC 113-2221-E-141-007-.

REFERENCES

[1] Inayatulloh, R. Toyib, E. Sahputra, Y. Reswan, Y. Darmi, and Meisyarah, "Adoption Block Chain Technology and Internet of Thing for Medical Record in Health Insurance," *13th International Conference on Information and Communication Technology Convergence*, Jeju Island, Korea, pp. 1539-1542, 2022.

[2] A. S. Pallivalappil, S. S. Ahmad, Y. Raju, C. K. Kumar, T. M. W, and N. Krishnaiah, "Applications of Ensuring Security and Privacy Using Block Chain with IoT for Health Record," *2nd International Conference on Advance Computing and Innovative Technologies in Engineering*, Greater Noida, India, pp. 1911-1917, 2022.

[3] J. V. Sagar, P. Siddharth, B. N. Sai, and U. Seshadri, "Automated Insurance Claims Using Block Chain," *10th International Conference on Advanced Computing and Communication Systems*, Coimbatore, India, pp. 98-102, 2024.

[4] I. Nath, "Data Exchange Platform to Fight Insurance Fraud on Blockchain," *IEEE 16th International Conference on Data Mining Workshops*, Barcelona, Spain, pp. 821-825, 2016.

[5] P. Varalakshmi, B. Sivasankari, R. A. Kumar, K. M. Nithish Kumar, and T. V. Venthan, "Development of Healthcare Insurance Claim Mechanism using Blockchain Technology," *1st International Conference on Computational Science and Technology*, Chennai, India, pp. 835-840, 2022.

[6] G. Singh, M. Sharma, S. Nanda, and S. Kadyan, "Disruptive Technologies and Digitalization in Insurance: Improving the Value Chain of Insurance," *3rd International Conference on Computation, Automation and Knowledge Management*, Dubai, United Arab Emirates, pp. 1-5, 2022.

[7] R. L. Neupane, E. Bonnah, B. Bhusal, K. Neupane, K. A. Hoque, and P. Calyam, "Formal Verification for Blockchain-based Insurance Claims Processing," *IEEE Network Operations and Management Symposium*, Seoul, Korea, pp. 1-5, 2024.

[8] U. Raghav, S. Singh, S. Setia, A. Anand, and N. Singh, "Optimizing Vehicle Insurance Claims: Streamlining Settlement Processes with Blockchain Technology," *First International Conference on Technological Innovations and Advance Computing*, Bali, Indonesia, pp. 11-18, 2024.

[9] M. Saddam and M. Ilyas, "Processing Health Insurance Claims Based on Blockchain Technology," *2nd International Conference on Computing and Machine Intelligence*, Istanbul, Turkey, pp. 1-5, 2022.

[10] H. Liu, S. Zhang, M. Ho, and P. Wang, "Research on the Application of Block-chain in Internet of Vehicles Insurance," *Management Science Informatization and Economic Innovation Development Conference*, Guangzhou, China, pp. 334-337, 2020.

[11] A. S. S Mishra, "Study on Blockchain-Based Healthcare Insurance Claim System," *Asian Conference on Innovation in Technology*, Pune, India, pp. 1-4, 2021.

[12] S. Khatri, F. A. Alzahrani, M. T. J. Ansari, A. Agrawal, R. Kumar, and R. A. Khan, "A Systematic Analysis on Blockchain Integration With Healthcare Domain: Scope and Challenges," *IEEE Access*, vol. 9, pp. 84666-84687, 2021.

[13] C. Zhu, J. Hu, J. Wu, C. Long, and X. Si, "A Blockchain-Based Accident Forensics System for Smart Connected Vehicles," *Proceedings of the 6th Blockchain and Internet of Things Conference*, ACM, New York, USA, pp. 128-136, 2024.

[14] A. Goyal, A. Elhence, V. Chamola, and B. Sikdar, "A Blockchain and Machine Learning based Framework for Efficient Health Insurance Management," *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*, ACM, New York, USA, pp. 511-515, 2021.

[15] W.-Y. Chiu and W. Meng, "Towards decentralized bicycle insurance system based on blockchain," *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, ACM, New York, USA, pp. 249-256, 2021.

Authors' background

Your Name	Title*	Research Field	Personal website
Chih-Chung Lin	Assistant Professor	RFID, IoT, AI, Security, Financial Technology	https://cin.lhu.edu.tw/p/404-1017-12810.php?Lang=zh-tw

Yuan-Cheng Lai	**Distinguished Professor**	**RFID, AI Network, AI FinTech, AI Network Security**	**https://www.cs.ntust.edu.tw/p/405-1102-105880,c10827.php?Lang=zh-tw**