BABEŞ-BOLYAI UNIVERSITY CLUJ-NAPOCA
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
SPECIALIZATION Software Engineering

DISSERTATION THESIS

Blockchain Technology in Insurance Industry

Supervisor
Prof. Dr. Motogna Simona

Author
Criste Denis Lorin

2023

ABSTRACT

Blockchain technology has disrupted various industries, and the insurance sector is no exception. The decentralized and immutable nature of blockchain makes it an ideal platform for insurers to improve their claims processing system. This dissertation thesis aims to explore the potential of blockchain technology in the insurance industry and develop a demo platform that uses smart contracts to facilitate and streamline the claims process.

The first chapter of this paper provides an overview of blockchain technology and its key features, including decentralization, transparency, and immutability. The second chapter explores the insurance industry, its challenges, and the potential benefits of using blockchain technology.

The third chapter presents the design and implementation of the demo platform, which uses Ethereum blockchain and smart contracts to facilitate the claims process. The platform allows users to submit claims and track the status of their claims in real-time. The smart contract ensures that the claims are processed efficiently and transparently.

The fourth chapter presents the results of the research conducted on the demo platform.

Overall, this dissertation thesis provides an in-depth analysis of the potential of blockchain technology in the insurance industry and demonstrates how a demo platform can be developed to improve the claims process using smart contracts. The research conducted on the platform provides insights into the benefits and limitations of using blockchain technology in the insurance industry.

This work is the result of my own activity. I have neither given nor received unauthorized assistance on this work.

Criste Denis Lorin

Contents

Chapter 1

Introduction

1.1 Background and Motivation

The insurance industry is a critical component of the modern economy, providing financial protection to individuals and businesses against various risks. However, the traditional insurance industry is often associated with long processing times, high administrative costs, and a lack of transparency. The emergence of blockchain technology has the potential to transform the insurance industry by addressing these challenges and providing more efficient and transparent insurance services.

In recent years, there has been a growing interest in the use of blockchain technology in the insurance industry. Several studies have explored the potential of blockchain technology to improve the claims processing system and enhance the customer experience. For example, Insurwave is a blockchain-based platform that offers marine insurance services. It uses blockchain technology to automate the claims process, providing real-time visibility and transparency to all parties involved. Another example is B3i, a consortium of insurers that have developed a blockchain-based platform to streamline the reinsurance process.

Motivated by the potential benefits of blockchain technology in the insurance industry, this dissertation thesis aims to develop a demo platform that uses smart contracts to streamline the claims process. The platform will allow users to submit claims and track the status of their claims in real-time, ensuring that the process is efficient and transparent. What will make this platform unique is its user-friendly interface and its ability to create personalized policies with a large range of customization. The research conducted on the demo platform will provide insights into the benefits and limitations of using blockchain technology in the insurance industry, and the potential for further development and adoption of blockchain-based insurance solutions.

Overall, this dissertation thesis builds upon previous research and aims to contribute to the growing body of knowledge on the use of blockchain technology in the insurance industry. The demo platform developed in this study has the potential to transform the insurance industry by providing a more efficient and transparent claims processing system, while also offering unique features that differentiate it from other blockchain-based insurance platforms.

1.2 Research questions and objectives

The main research questions of this study are:

1. How can blockchain technology improve the efficiency and transparency of the insurance industry? This question explores the key features of blockchain technology that make it suitable for the insurance industry, such as its ability to help reduce fraud, enhance data security, and streamline claims processing in the insurance sector.

2. What are the key features of smart contracts that can benefit insurance processes? This question focuses on how smart contracts can enable automation and reduce the need for intermediaries in insurance operations. It also investigates the potential applications of smart contracts in various insurance segments, such as life, health, property, and casualty insurance.

3. How can a decentralized insurance platform be designed and implemented using blockchain technology? This question delves into the key components and architecture of a decentralized insurance platform. It examines how smart contracts can be integrated into the platform to facilitate automation and improve customer experience.

4. What are the challenges and limitations of implementing blockchain technology in the insurance industry? This question aims to assess the technical, legal, regulatory, and ethical challenges of implementing blockchain technology in the insurance industry. It also examines potential solutions to address these challenges and facilitate the adoption of blockchain technology.

5. How can blockchain technology foster innovation and collaboration in the insurance industry? This question investigates the role of blockchain technology in enabling the development of new, customer-centric insurance products and services. It also analyzes the impact of blockchain technology on emerging insurance models, such as peer-to-peer insurance and parametric insurance.

The objectives of this study are:

1. To provide an in-depth understanding of blockchain technology, its key components, consensus mechanisms, and potential applications in the insurance industry. This objective includes a review of the literature on blockchain technology and

its underlying principles, as well as an exploration of the various consensus mechanisms used in blockchain networks and their implications for the insurance sector.

2. To analyze the functionality of smart contracts and their potential applications in the insurance industry. This objective aims to examine the features of smart contracts that make them suitable for automating insurance processes and to investigate the use of smart contracts in different insurance segments and their potential impact on cost reduction, efficiency, and customer satisfaction.

3. To develop a practical decentralized insurance platform that demonstrates the use of blockchain technology and smart contracts to streamline insurance processes and improve customer experience. This objective involves designing the architecture and key components of a decentralized insurance platform using blockchain technology, implementing smart contracts for various insurance processes such as policy issuance, claims processing, and premium payment, and evaluating the platform's performance in terms of efficiency, security, and user experience.

4. To identify the challenges and opportunities for integrating blockchain technology into insurance processes. This objective seeks to assess the technical, legal, regulatory, and ethical challenges of implementing blockchain technology in the insurance industry and to examine potential solutions that can address these challenges and facilitate the adoption of blockchain technology.

5. To explore the potential of blockchain technology to foster innovation and collaboration in the insurance industry. This objective investigates the role of blockchain technology in enabling the development of new, customer-centric insurance products and services, as well as its impact on emerging insurance models such as peer-to-peer insurance and parametric insurance.

By addressing these research questions and objectives, this study aims to contribute to the understanding of blockchain technology's potential in transforming the insurance industry and provide a roadmap for future research and practical applications.

1.3 Overview of the insurance industry and current challenges

The insurance industry plays a crucial role in providing financial protection against risks and uncertainties. It consists of various segments, such as life insurance, property and casualty insurance, and health insurance. However, the industry faces several challenges, including:

Inefficiencies in claims processing: Manual and paper-based processes lead to delays, high costs, and poor customer experience. Fraudulent claims: The lack of a transparent and tamper-proof system makes it difficult to identify and prevent fraudulent claims. Data security and privacy concerns: The centralized nature of traditional insurance systems exposes sensitive customer data to risks of hacking and data breaches. Limited innovation and customer-centric products: Legacy systems and regulations hinder the development of new, personalized insurance products and services.

1.4 Previous research and existing applications

Numerous studies have explored the potential applications of blockchain technology in the insurance industry. Researchers have identified various use cases, such as streamlining claims processing, improving data security, and enabling peer-to-peer insurance models. Some notable examples of blockchain-based insurance applications include:

- **Etherisc**: Etherisc [eth23] is a decentralized insurance platform that focuses on automating the process of buying and claiming flight delay insurance using smart contracts. When a user purchases flight delay insurance on the Etherisc platform, a smart contract is created that includes the terms and conditions of the policy. The smart contract is then connected to external data sources, such as flight data APIs, which provide real-time information about flight statuses. In the event of a flight delay that meets the criteria specified in the policy, the smart contract automatically executes and compensates the insured party without the need for any manual intervention. This approach significantly streamlines the claims process, reduces the potential for fraud, and enhances the overall customer experience.

- **Fizzy AXA**: Fizzy AXA [fiz23] is a parametric insurance product developed by AXA, a leading global insurance company. The product offers automatic compensation for flight delays through smart contracts on the Ethereum blockchain. Similar to Etherisc, Fizzy AXA relies on external data sources to monitor flight statuses and trigger compensation when the conditions specified in the policy are met. By using smart contracts and blockchain technology, Fizzy AXA eliminates the need for manual claims processing and reduces the time it takes for customers to receive compensation. Additionally, the transparent nature of the blockchain ensures that customers can trust the process and have full visibility into the status of their claims.

- **Insurwave**: Insurwave [ins23] is a blockchain-based platform designed for marine insurance, aiming to revolutionize the way insurance is managed in the shipping industry. The platform enables real-time sharing of data and automation of processes, which results in reduced administrative costs and improved risk management. Insurwave connects various stakeholders, such as insurers, reinsurers, brokers, and shipping companies, on a single, decentralized platform that facilitates secure data sharing and collaboration. By leveraging blockchain technology, Insurwave ensures data integrity and transparency, enabling stakeholders to make more informed decisions and optimize their risk management strategies. Furthermore, the platform uses smart contracts to automate key insurance processes, such as policy issuance and claims handling, which significantly improves efficiency and reduces the potential for human error.

These applications demonstrate the potential of blockchain technology and smart contracts to revolutionize the insurance industry by addressing existing challenges and unlocking new opportunities.

Chapter 2

Blockchain Technology: An Overview

2.1 Introduction

Blockchain technology has emerged as a groundbreaking innovation with the potential to disrupt various industries and transform traditional business processes. Although initially developed to support cryptocurrencies like Bitcoin, blockchain technology has since demonstrated its potential to revolutionize other sectors, including finance, supply chain management, healthcare, and insurance [TT16, Mou16]. The decentralized, transparent, and immutable nature of blockchain technology makes it an ideal platform for insurers to improve their claims processing system and enhance customer trust.

This chapter provides an overview of blockchain technology, its key features, and its potential applications in various industries, with a focus on the insurance sector. We will discuss the fundamental principles of blockchain technology, including its architecture, consensus mechanisms, and the concept of smart contracts. Furthermore, we will examine the challenges and limitations that need to be addressed for the widespread adoption and implementation of blockchain technology in various industries.

2.2 Blockchain Technology: Fundamentals

Blockchain is a decentralized, distributed ledger technology (DLT) that enables secure and transparent transactions between parties without the need for intermediaries, such as banks or other central authorities [NBF+16]. The term "blockchain" refers to the structure of the technology, which consists of a chain of blocks containing transaction data. Each block is cryptographically linked to the previous block, ensuring that the data stored on the blockchain is tamper-proof and immutable.

2.2.1 Blockchain Architecture

A blockchain network consists of multiple nodes, or computers, that maintain a copy of the ledger and participate in the validation of transactions. When a new transaction is initiated, it is broadcast to all nodes in the network. The nodes then use consensus algorithms to agree on the validity of the transaction and add it to a new block. Once a block is filled with a certain number of transactions, it is added to the chain, creating a permanent and unchangeable record of the transaction data.

2.2.2 Types of Blockchain Networks

There are three main types of blockchain networks: public, private, and consortium. Each type has its unique characteristics and is suited for different applications and industries.

- **Public Blockchains:** These are open, decentralized networks that allow anyone to participate in the transaction validation process and maintain a copy of the ledger. Public blockchains are secured by consensus algorithms, such as Proof of Work (PoW) or Proof of Stake (PoS), which ensure the integrity of the data and prevent malicious actors from tampering with the ledger. Examples of public blockchains include Bitcoin and Ethereum.

- **Private Blockchains:** In contrast to public blockchains, private blockchains are closed networks that restrict participation to specific, pre-approved entities. Private blockchains are often used by organizations to improve internal processes and maintain greater control over their data. They typically employ a different consensus mechanism, such as Practical Byzantine Fault Tolerance (PBFT), which requires less computational power and provides faster transaction processing times.

- **Consortium Blockchains:** These are hybrid networks that combine aspects of both public and private blockchains. Consortium blockchains are typically governed by a group of trusted organizations that share the responsibility of validating transactions and maintaining the ledger. This type of blockchain is well-suited for industries that require collaboration between multiple stakeholders, such as supply chain management or interbank transactions.

2.2.3 Consensus Mechanisms

In a decentralized network like blockchain, there is no central authority to decide which transactions are valid and which are not. Instead, multiple nodes in the network must reach an agreement on the validity of transactions and the order in which they are added to the blockchain. This process is known as consensus.

Consensus mechanisms are the algorithms used by blockchain networks to agree on the validity of transactions and maintain the integrity of the ledger. They play a critical role in ensuring the security and reliability of the blockchain [Vis21]. There are several consensus mechanisms used in blockchain networks, with the most common ones being Proof of Work (PoW) and Proof of Stake (PoS).

Proof of Work (PoW) is the first and most well-known consensus algorithm, pioneered by Bitcoin. It requires miners to solve complex mathematical puzzles to validate and add new transactions to the blockchain. The process of solving these puzzles consumes a significant amount of computational power and energy, making it costly and time-consuming for potential attackers to manipulate the network.

PoW operates on the principle that the more work a participant invests in validating transactions, the more likely they are to be chosen to add a new block to the blockchain. Once a miner solves the puzzle, they broadcast their solution to the network, and other miners verify the correctness of the solution. If a majority of miners agree, the block is added to the blockchain, and the successful miner is rewarded with newly minted cryptocurrency and transaction fees.

While PoW has proven to be secure and effective, it has some drawbacks, including high energy consumption, the potential for centralization due to specialized mining hardware, and slow transaction processing times. These limitations have prompted the development of alternative consensus mechanisms.

Proof of Stake (PoS) is an alternative consensus algorithm designed to address some of the issues associated with PoW. Instead of relying on computational power to secure the network, PoS uses the amount of cryptocurrency held by participants (their ”stake”) as a measure of their influence in the network. The more cryptocurrency a participant holds, the higher their chances of being selected to validate transactions and add new blocks to the blockchain.

In PoS, participants ”lock” a portion of their cryptocurrency holdings in a wallet to show their commitment to the network. The algorithm then selects validators based on the size of their stake and other factors, such as the length of time they have held the cryptocurrency. Validators are responsible for validating transactions and adding new blocks to the blockchain. In return, they receive transaction fees and, in some cases, newly minted cryptocurrency as a reward.

PoS offers several advantages over PoW, including reduced energy consumption, faster transaction processing times, and a more decentralized network. However, it also introduces new challenges, such as the potential for ”nothing at stake” attacks and the risk of centralization due to large stakeholders dominating the validation process.

Delegated Proof of Stake (DPoS) is a variation of the PoS consensus algorithm that aims to further improve network efficiency and decentralization. In DPoS, network participants elect a small number of trusted validators, known as delegates, to validate transactions and maintain the blockchain on their behalf. Delegates are chosen based on their reputation, performance, and the amount of cryptocurrency staked by their supporters.

DPoS offers several benefits over traditional PoS, including faster transaction processing times, greater scalability, and improved decentralization. By allowing network participants to vote for their preferred delegates, DPoS ensures that power is more evenly distributed among the community and reduces the risk of centralization. Additionally, delegates are incentivized to act in the best interests of the network, as their reputation and rewards depend on their performance and the support of the community.

However, DPoS also has its challenges, such as the potential for collusion between delegates, the risk of centralization if a small group of delegates gains too much power, and the reliance on voting participation by network participants to maintain decentralization.

2.2.4 Smart Contracts

Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They automatically execute predefined actions when specific conditions are met, eliminating the need for intermediaries and reducing the potential for human error or fraud. Smart contracts are stored on the blockchain, ensuring their transparency, immutability, and security. [Coi21]

Smart contracts are created using programming languages like Solidity (for Ethereum) or Cadence (for Flow). The code defines the terms and conditions of the agreement, as well as the actions to be taken when specific conditions are met. Once the code is written, the smart contract is deployed on the blockchain, where it becomes immutable and transparent.

Users can interact with smart contracts by sending transactions to the contract's address on the blockchain. These transactions can trigger the execution of the contract's code based on the predefined conditions. For example, a user might send a transaction to a smart contract to purchase an insurance policy, which would then automatically issue the policy and store the relevant information on the blockchain.

Smart contracts have a wide range of applications across various industries. In the insurance industry, smart contracts can automate claims processing, ensuring that payouts are made promptly and accurately when a qualifying event occurs. They can also enable decentralized risk assessment and streamline premium payments. Smart contracts can also be used in Supply Chain Management. They can track and verify the movement of goods throughout the supply chain, ensuring transparency and reducing fraud. They can also automate payments between parties, improving efficiency and reducing the potential for disputes. Financial Services is the industry where smart contracts had the biggest impact. Smart contracts can facilitate the creation of decentralized finance (DeFi) platforms, enabling users to borrow, lend, or trade assets without relying on traditional financial institutions. They can also be used to create complex financial instruments, such as derivatives and prediction markets. Finally, smart contracts can facilitate decentralized voting systems, ensuring transparency and immutability in decision-making processes. They can also be used to create decentralized autonomous organizations (DAOs), which are organizations run entirely through smart contracts and governed by their stakeholders.

The process of developing and deploying smart contracts typically involves the following steps: design, coding, testing, auditing, and deploying.

Before writing any code, it is important to carefully define the desired functionality and behavior of the smart contract. This includes specifying the terms and conditions of the agreement, as well as any inputs, outputs, or events that the contract will handle. Once the design is complete, the developer can begin writing the smart contract code using a programming language like Solidity. This involves defining functions, variables, and data structures that will implement the contract's logic. After writing the code, the developer must thoroughly test the smart contract to ensure it behaves as expected and to identify any potential security vulnerabilities. This can be done using unit tests, integration tests, and manual testing on testnet environments. Once the smart contract has been tested and audited, it can be deployed to the mainnet. This involves sending a transaction to the blockchain that includes the compiled smart contract code and any necessary configuration data. Once the transaction is confirmed, the smart contract is considered to be live and can be interacted with by users.

As the blockchain ecosystem continues to expand, the need for interoperability between different networks and platforms becomes increasingly important. Interoperability can enable seamless communication and value transfer between various blockchain networks, allowing users to more easily access and utilize diverse applications and services.

Some emerging technologies and initiatives that aim to improve interoperability in the blockchain space include: Cross-Chain Bridges, Interchain Communication Protocols, Multi-Chain Wallets and Exchanges, Standardized token formats

Cross-Chain Bridges are mechanisms that enable the transfer of assets or data between different blockchain networks. Cross-chain bridges can be built using various techniques, such as atomic swaps, decentralized relays, or multi-chain smart contracts.

Interchain Communication Protocols are standardized protocols that facilitate communication between different blockchain networks. Examples include the Inter-Blockchain Communication (IBC) protocol developed by the Cosmos project and the Polkadot Substrate framework, which allows for cross-chain message passing.

Wallets and exchanges that support multiple blockchain networks can help improve interoperability by allowing users to easily manage and trade assets across various platforms.

Standardized token formats, such as the ERC-20 standard for Ethereum, can help ensure compatibility between different blockchain networks and make it easier for users to interact with various applications and services.

2.3 Web 3.0 and the Decentralized Web

The ongoing evolution of the Internet is characterized by the transition from Web 2.0 to Web 3.0, often referred to as the decentralized or semantic Web. The journey from the early days of the internet (Web 1.0), which was largely read-only, to Web 2.0, which brought interactivity and the rise of social media, has now led to Web 3.0, a new phase promising a highly decentralized and semantically intelligent internet [HHSBL08].

Web 3.0 is often associated with blockchain technology and its ability to facilitate decentralized networks. This includes a more user-centric web experience, with greater privacy, control over one's own data, and direct peer-to-peer interactions without the need for intermediaries.

2.3.1 Understanding Web 3.0

Web 3.0 aims to create a smarter and more connected web, where machines can read and understand the content, context, and users' intentions just as human beings do. The semantic web will enable better content delivery, more relevant information, and an enhanced browsing experience.

The vision of Web 3.0 includes:

Semantic Web: Using metadata and ontologies to understand and connect the meaning of data, the semantic web enables machines to process and understand the data that they merely display in Web 2.0.

Intelligent Agents: In a semantic web, intelligent agents will be able to understand and process information independently, assisting users in finding the most relevant information based on their preferences and needs.

Interoperability: Web 3.0 envisions a highly interoperable web where data from various sources and formats can be integrated seamlessly. This is enabled by standard formats and protocols that facilitate data exchange and integration.

Decentralization: In contrast to the centralized structures of Web 2.0, where a few large platforms control vast amounts of data, Web 3.0 envisions a decentralized web where users control their own data. Blockchain is one of the key technologies driving this shift towards decentralization.

2.3.2 The Role of Blockchain in Web 3.0

Blockchain technology is a key component of the shift towards Web 3.0. Its decentralized, transparent, and secure nature aligns perfectly with the vision of a user-centric and privacy-focused web [TT16].

Here are a few ways blockchain is contributing to the evolution of the Web 3.0:

Decentralization: One of the core values of Web 3.0 is decentralization, and blockchain is inherently decentralized. This means that control is distributed among many nodes in the network, rather than being concentrated in a central authority. This can help prevent censorship and ensure that no single entity can control or manipulate the network.

Data Ownership: Blockchain technology allows users to maintain control of their own data, including their digital identities. This is a significant shift from the current web, where users often surrender their data to large platforms in exchange for free services. With blockchain, users can choose when and how to share their data, and even monetize it if they choose.

Smart Contracts: These are self-executing contracts with the terms of the agreement directly written into code. They are stored on the blockchain and automatically execute actions when certain conditions are met. This can automate a wide range of interactions on the web, reducing the need for intermediaries and making processes more efficient and transparent.

Interoperability: Blockchain networks can be designed to interoperate, allowing for seamless interactions and transactions across different blockchains. This is a key feature of Web 3.0, enabling a more connected and integrated Web 3.0, commonly referred to as the decentralized web or the semantic web, is the third generation of Internet services that uses artificial intelligence, blockchain technology, and decentralized networks to create a more connected and intelligent web experience. Unlike Web 2.0, which is largely centralized and controlled by a few large corporations, Web 3.0 emphasizes decentralization, user control, and privacy, powered by distributed ledger technology (DLT) like blockchain [Fou22].

2.3.3 Features of Web 3.0

Web 3.0 is characterized by several key features, including:

Decentralization: One of the most significant features of Web 3.0 is its decentralized nature. This is primarily achieved through the use of blockchain technology, which eliminates the need for centralized intermediaries and enables peer-to-peer interactions. This decentralization allows for greater user control over data and improves system resiliency against attacks or outages.

Semantic Web: Web 3.0 aims to create a "semantic web", where data and information are linked in meaningful ways. This semantic structure enables better data interoperability, as different applications and services can understand and process the data more effectively. It also allows for more advanced search capabilities and AI-powered data analysis.

Interoperability: Web 3.0 focuses on building a network of interconnected blockchains that can communicate with each other seamlessly. This cross-chain interoperability allows for a more fluid exchange of data and value across different blockchain networks and platforms, increasing the utility and accessibility of various decentralized applications (dApps) and services.

Privacy and Security: Through the use of cryptographic algorithms, blockchain technology provides improved security for Web 3.0. It allows users to have full control over their data, with the ability to dictate who can access it and under what circumstances. Additionally, the inherent transparency of blockchains helps foster trust among network participants.

2.3.4 Impact of Blockchain on Web 3.0

Blockchain technology is integral to the development of Web 3.0. It provides the foundational infrastructure for creating a decentralized and secure web where users have full control over their data.

Decentralized Applications (dApps): One of the most significant contributions of blockchain to Web 3.0 is the concept of decentralized applications (dApps). Unlike traditional applications, dApps run on decentralized networks, removing the need for a central authority or intermediary. This gives users greater control over their interactions and reduces reliance on third-party service providers.

Smart Contracts: Smart contracts are programmable scripts that automate the execution of transactions when predetermined conditions are met. They serve as the backbone of many dApps, facilitating complex interactions on the blockchain. Smart contracts enable the creation of decentralized platforms for finance (DeFi), supply chain management, gaming, and many other industries on Web 3.0.

Decentralized Identity and Data Sovereignty: Blockchain technology enables the creation of decentralized identity systems, where users have complete control over their personal data. This concept, known as data sovereignty, is a core principle of Web 3.0. It enables users to control who can access their data, how it is used, and even monetize it if they choose.

Token Economy: The tokenization of assets and activities is a key aspect of blockchain's impact on Web 3.0. Tokens can represent ownership or access rights, incentivize participation in network activities, or serve as a medium of exchange within dApps. This token economy can enable new business models and value creation opportunities in the Web 3.0 ecosystem.

2.3.5 Challenges and Future of Web 3.0 and Blockchain

Despite its potential, Web 3.0, powered by blockchain technology, still faces significant challenges:

Scalability: One of the main challenges for blockchain is scalability. As the number of transactions increases, the network becomes slower and more expensive to use. Various solutions, such as sharding or Layer 2 solutions, are being developed, but these are still works in progress and come with their own challenges.

User Experience (UX): While blockchain-based dApps offer more control and privacy, they often lack the user-friendly interfaces found in traditional apps. This can be a barrier to adoption for non-technical users.

Regulation: As a relatively new and disruptive technology, blockchain often falls into regulatory grey areas. This uncertainty can hinder development and adoption, especially in industries like finance where regulatory compliance is crucial.

Interoperability: While cross-chain interoperability is a key goal of Web 3.0, achieving it is easier said than done. Different blockchain networks have different protocols, standards, and security models, making it challenging to enable seamless communication between them.

Privacy vs. Transparency: Blockchain's transparency is a double-edged sword. While it can foster trust and accountability, it can also lead to privacy concerns if sensitive data is exposed on the public ledger.

Despite these challenges, the potential of a decentralized, user-centric, and intelligent web is attracting significant interest and investment. Web 3.0, powered by blockchain, could transform various industries, from finance to supply chain management, gaming, social media, and more. It promises a future where users are in control of their data, where digital interactions are secure and trustless, and where online communities can govern themselves through decentralized autonomous organizations (DAOs).

The road to Web 3.0 might be challenging, but its potential makes it an exciting area of innovation for the next decade and beyond.

2.4 Challenges and Limitations of Blockchain Technology

Despite its transformative potential, blockchain technology also faces several challenges and limitations that need to be addressed for its widespread adoption and implementation in various industries, including insurance. Among these challenges, the most important are scalability, privacy, interoperability, energy consumption, and legal and regulatory uncertainty.

One of the main challenges facing blockchain technology is its scalability. As the number of transactions and participants in a network increases, the processing time and resources required to maintain the blockchain also increase. This can lead to slower transaction processing times and higher fees, limiting the technology's suitability for large-scale applications [CDE+16].

While transparency is a key feature of blockchain technology, it can also raise privacy concerns, particularly in industries that deal with sensitive information, such as insurance and healthcare. Public blockchains, by their nature, make transaction data visible to all participants, which may not always be desirable. Private and consortium blockchains offer more control over data access, but they may not provide the same level of decentralization and security as public blockchains [Zoh15].

As the number of blockchain platforms and applications grows, there is a need for interoperability between different networks to enable seamless data exchange and collaboration. Currently, most blockchain platforms operate in isolation, limiting their potential for integration with existing systems and other blockchain networks. Several initiatives, such as the Interledger Protocol (ILP) and the Polkadot network, aim to address this issue by facilitating cross-chain communication and data transfer [TS18, Woo19].

The legal and regulatory landscape for blockchain technology is still evolving, with many jurisdictions yet to establish clear guidelines and frameworks for its use. This uncertainty can hinder the adoption of blockchain technology in industries that are heavily regulated, such as insurance and finance. Policymakers and regulators need to develop comprehensive, technology-neutral regulations that address potential risks while fostering innovation and growth in the blockchain ecosystem [GM19].

Proof of Work (PoW), the consensus algorithm used in many public blockchains, such as Bitcoin and Ethereum, is known for its high energy consumption. The environmental impact of PoW has led to calls for more sustainable consensus algorithms, such as Proof of Stake (PoS), which are being increasingly adopted by newer blockchain platforms [But14]. However, transitioning existing networks to more energy-efficient consensus mechanisms can be a complex and challenging process.

2.5 Conclusion

This chapter has provided an overview of blockchain technology, its key features, and its potential to transform various industries, including insurance. By understanding the fundamentals of blockchain technology and its unique characteristics, such as decentralization, transparency, and immutability, readers can better appreciate how blockchain can revolutionize traditional processes in the insurance industry and create more efficient, secure, and transparent systems.

In the subsequent chapters, we will delve deeper into the insurance industry, exploring its current challenges and the potential benefits of implementing blockchain technology to address these issues. We will also discuss the concept of smart contracts and their applications in automating insurance claims processing, followed by the design and implementation of a demo platform that uses blockchain and smart contracts to streamline the claims process.

Chapter 3

Practical Application

This chapter aims to provide an in-depth analysis of the demo platform developed in this study, which utilizes blockchain technology and smart contracts to streamline the claims process.

In addition, this chapter will explore the potential of blockchain technology and smart contracts in the insurance industry, particularly in the context of Web3. Web3 refers to the next generation of the internet, which is decentralized and peer-to-peer, allowing for greater transparency, security, and privacy. The integration of blockchain technology and smart contracts with Web3 has the potential to transform the insurance industry by creating a more decentralized and democratic ecosystem.

Overall, this research chapter will provide insights into the potential of blockchain technology and smart contracts in the insurance industry, and the effectiveness of the demo platform developed in this study in streamlining the claims process. The chapter will also explore the potential of Web3 in the insurance industry, highlighting the benefits and challenges of integrating blockchain technology and smart contracts with the decentralized Web3 ecosystem.

3.1 Introduction to InsuranceChain

InsuranceChain is a demo insurance platform that will demonstrate some of the advantages of blockchain technology. Leveraging the power of blockchain technology, InsuranceChain aims to create a more transparent, efficient, and secure insurance ecosystem.

At its core, InsuranceChain focuses on streamlining key processes such as policy purchase and management, claims submission and tracking, and risk assessment. By automating these processes using smart contracts, InsuranceChain ensures that clients enjoy a seamless and user-friendly experience while benefiting from lower operational costs, faster claims processing, and increased transparency.

InsuranceChain's platform offers a wide range of features and use cases, enabling clients to easily create custom insurance policies, purchase and manage their policies, and submit and track claims in real-time. InsuranceChain is able to provide personalized risk assessments and pricing based on clients' unique risk profiles, potentially leading to more accurate pricing and lower premiums.

3.2 InsuranceChain Architecture

The InsuranceChain architecture involves three primary components: a smart contract deployed on the Ethereum testnet network "Sepolia", a backend service written in Node.js, and a frontend client application built using React. This combination forms a robust decentralized application (dApp) architecture that allows users to interact with a blockchain-based insurance system. 3.1

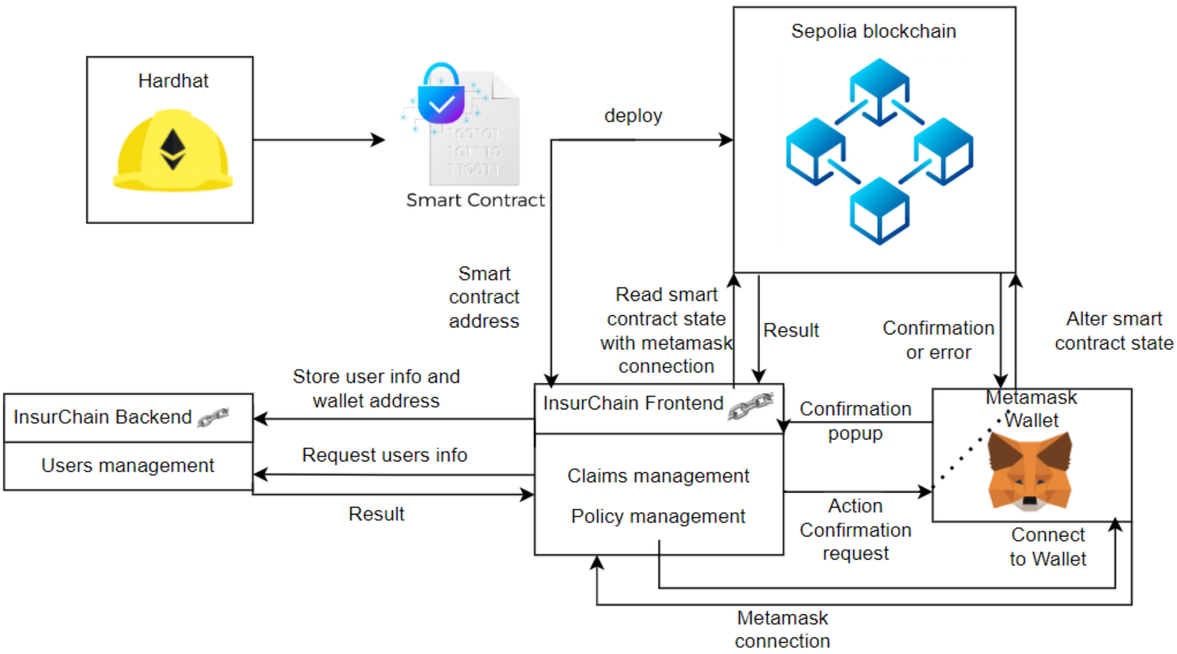

Figure 3.1: Architecture diagram

The smart contract in the insurance application is written in Solidity, a high-level, statically-typed programming language designed for developing smart contracts that run on the Ethereum Virtual Machine (EVM). Solidity's syntax is similar to that of JavaScript, making it relatively easy to learn for developers coming from a web development background.

```
function fileClaim(
    uint256 policyId,
    string memory description,
    uint256 amount
) public {
    require(policyId<policyCounter, "Policy Id is out of range.");
    require(policies[policyId].isAccepted, "Policy is not accepted.");
    require(policies[policyId].insured == msg.sender, "Only the insured can file a claim.");
    require(block.timestamp < policies[policyId].creationTime + policies[policyId].duration, "Policy is expired");
    require(policies[policyId].premiumDueDate > block.timestamp, "Premium must be paid before filing a claim.");
    require(amount <= policies[policyId].coverageAmount, "Claim exceeds coverage amount.");

    Claim memory newClaim;

    uint256 claimId = policyClaimCounters[policyId]++;
    newClaim.id = claimId;
    newClaim.description = description;
    newClaim.amount = amount;
    newClaim.isAccepted = false;
    newClaim.isAnswered = false;
    newClaim.policyId = policyId;
    newClaim.policyName = policies[policyId].policyName;
    policyClaims[policyId].push(newClaim);

    emit ClaimFiled(newClaim.id ,policyId, description, amount);
}
```

Figure 3.2: Smart contract method

This smart contract embodies the core business logic of the insurance system, encapsulating the rules for policy registration, policy management, and claims processing. This system architecture employs 'require' statements within the smart contract methods, ensuring the enforcement of these rules. 'Require' statements are a feature in smart contracts that allows for conditions to be validated before executing the contract's code. If the conditions in these statements aren't met, the smart contract reverts the transaction, thereby ensuring all operations align with the predefined rules. By encoding these rules and validation mechanisms into the smart contract, the system ensures that all transactions abide by these predefined rules. This leads to a trustworthy and transparent operation.

The smart contract is deployed on the Ethereum test network, Sepolia. Using a test network for deployment enables testing and refinement of the smart contract logic before it goes live on the Ethereum main network. This approach reduces the risks associated with smart contract development, as bugs or issues can be addressed without real-world financial implications.

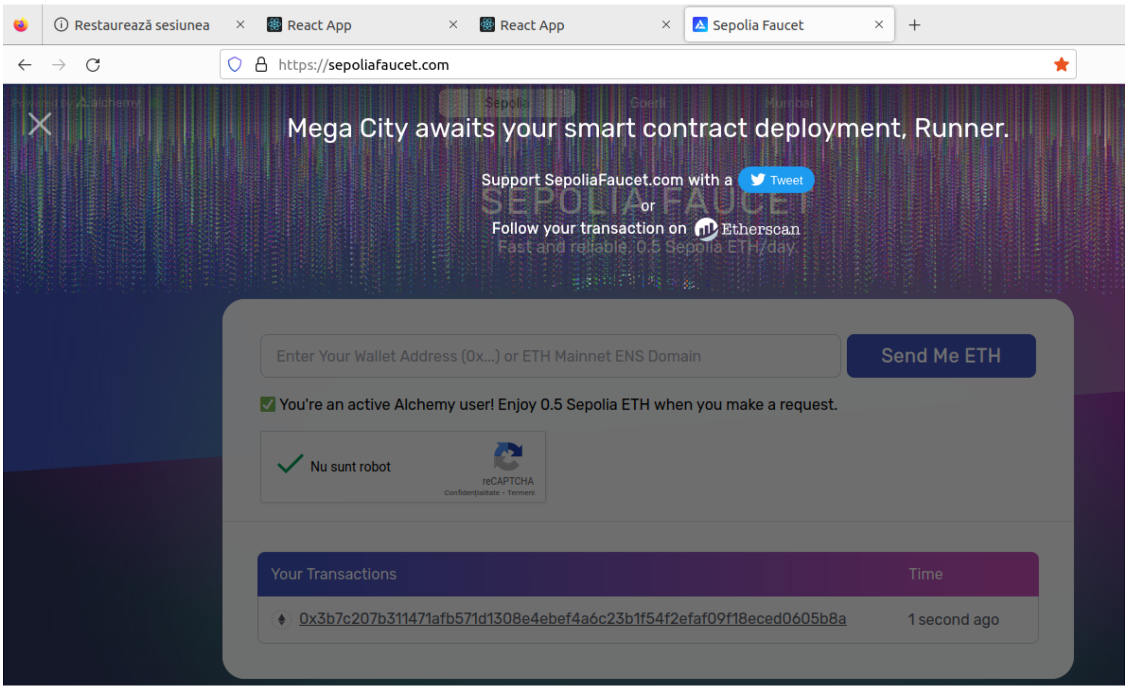

Figure 3.3: Sepolia faucet

For the development process, the Sepolia faucets are being utilized to receive Sepolia Ethereum coins. Faucets like Sepolia offer developers a valuable resource by providing free coins for use in testing and development environments. These coins fuel the development, testing, and fine-tuning of the smart contract, helping to ensure its smooth and reliable operation once deployed on the main Ethereum network. The combination of rigorous rule enforcement via 'require' statements, and the use of Sepolia Ethereum for development, contributes to the overall trustworthiness and transparency of our insurance system.

Hardhat is the tool utilized for the deployment and management of the smart contract. It is a development environment for Ethereum that aids in tasks such as compiling Solidity code, testing, and deploying contracts. It provides functionalities like console.log for Solidity and a powerful debugger, which can be invaluable for testing and development.

The backend server is responsible for managing user registrations and logins. It stores crucial information such as the user's wallet address, username, password, ID, and role. This separation of user management from the frontend adds an extra layer of security, as the backend server can be more tightly controlled and secured than the client-facing frontend.

Within this setup, the backend server plays an even more significant role in enhancing user experience and interaction. Besides managing user registrations and logins, it also serves as the repository to map wallet addresses to usernames. This mapping is a crucial feature as it allows users to see who they are interacting with, without needing to remember or recognize their wallet addresses.

The system retrieves the usernames associated with wallet addresses and presents them on the frontend application. This user-friendly approach not only simplifies navigation and interaction for users but also promotes a sense of community within the platform. Users can therefore engage with the insurance policies and claims more personally, knowing exactly who they are dealing with at every step of the process.

The frontend application, on the other hand, directly communicates with the smart contract. It uses the MetaMask browser extension to provide an Ethereum wallet and blockchain connection. Through a custom React hook utilizing the useEffect function, we set up an Ethereum provider using ethers.js's BrowserProvider tied to window.ethereum, which is injected by MetaMask.

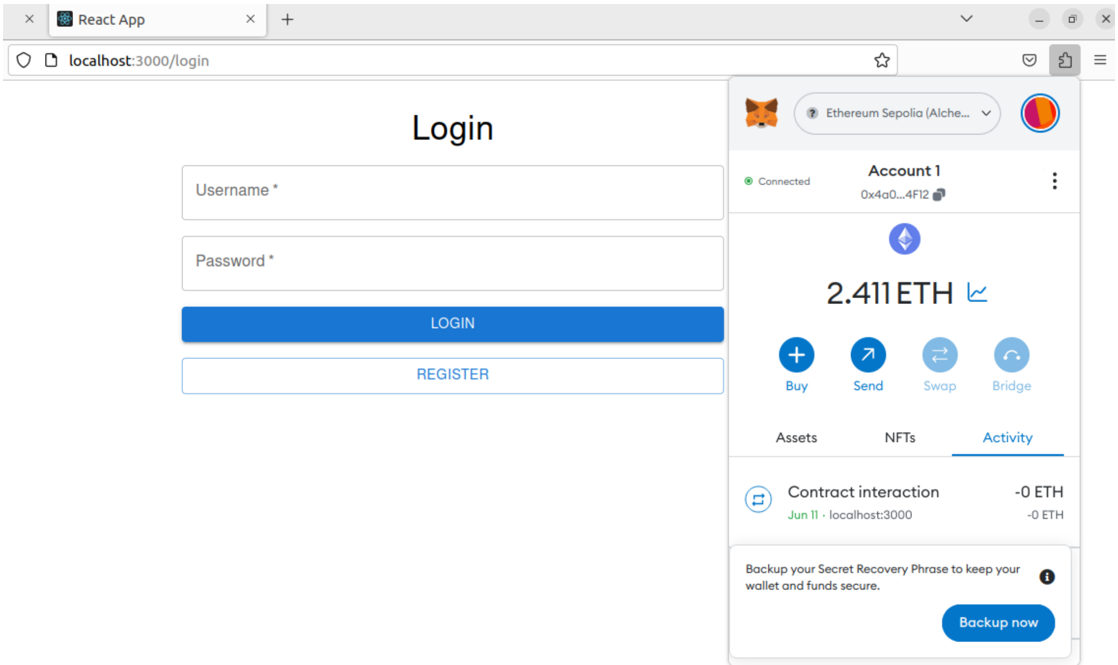

Figure 3.4: Metamask connection

The code then requests the user's accounts from the MetaMask wallet, and if successful, it obtains the signer corresponding to the provided address. The signer is an ethers.js abstraction used to perform actions that require a wallet, such as signing transactions. Using this signer, we instantiate a new contract instance using the address of the deployed contract and the ABI of the InsurancePolicy contract.

```
useEffect( effect: () : undefined | () => void  => {
    if (!isAuthenticated || address === null) return;

    // Get provider and setup initial contract
    // @ts-ignore
    const provider : ethers.BrowserProvider  = new ethers.BrowserProvider(window.ethereum);
    provider.send( method: "eth_requestAccounts",  params: []).then(
        _ => provider.getSigner(address).then(signer : ethers.JsonRpcSigner  =>
            setContract(new ethers.Contract(contractAddress, InsurancePolicy__factory.abi, signer)))
    ).catch(err => {
        console.error('Failed to request accounts:', err);
    });
```

Figure 3.5: Contract creation

We also set up an event listener to handle account changes. If the account in use changes, we obtain a new signer for the new account and use it to set up a new contract instance. This allows the frontend to react dynamically to account changes, ensuring it always interacts with the smart contract using the correct account.

Our frontend application is designed with usability in mind, presenting users with several interactive screens. These include a Policy table screen enabling users to manage their policies efficiently, a Claims table screen handling the management of claims, and a Create Policy page exclusive for insurers.

The separation of these interfaces offers an intuitive user experience. Insurers can create policies with ease, while policyholders have straightforward, dedicated interfaces for managing their policies and claims.

Combining the powerful capabilities of smart contracts with the user-friendly interface, our application provides a robust, efficient, and secure platform for all stakeholders in the insurance process.

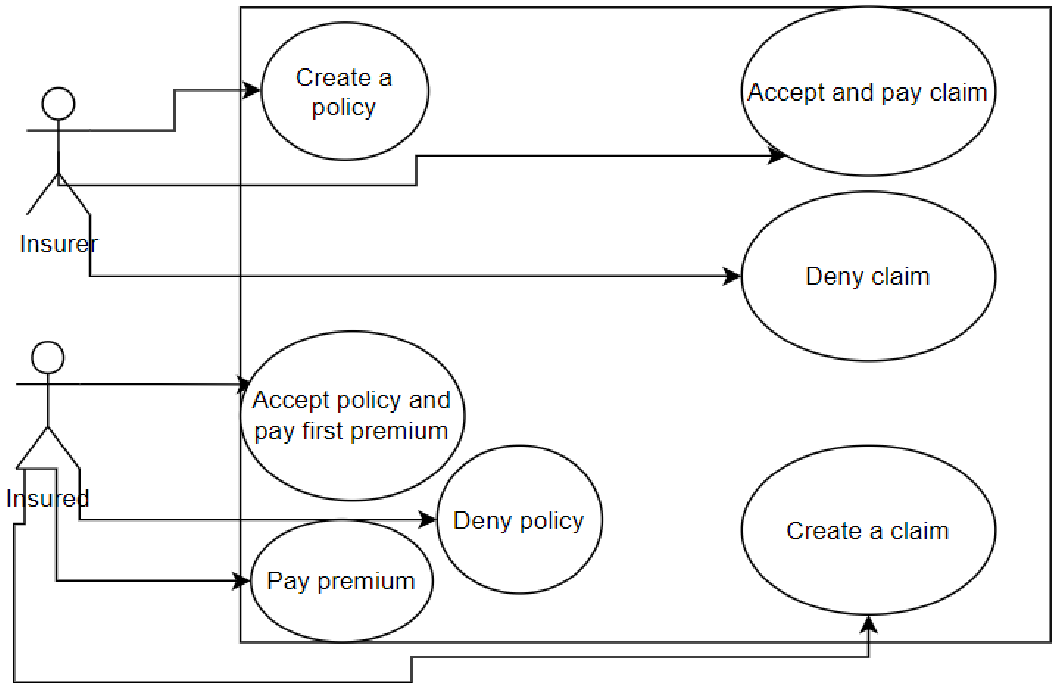

Figure 3.6: User roles

Our system leverages the power of blockchain to model a comprehensive insurance system involving two primary roles: Insurer and Insured. Each role has distinct responsibilities and capabilities within the platform.

Insurer: The insurer is responsible for creating insurance policies. A policy is created by providing a policy name, a description, and the name of the insured (selected from a dropdown). The insurer also assesses the risk associated with the insured – this could be based on various factors like age, health condition, occupation, etc. This risk assessment, although not stored, is vital in the determination of premium values. The insurer also sets the policy duration and the premium payment frequency.

Insured: The insured, on the other hand, interacts with these policies. They receive policy requests and can choose to accept or deny them. They are also responsible for filing claims against active policies when necessary.

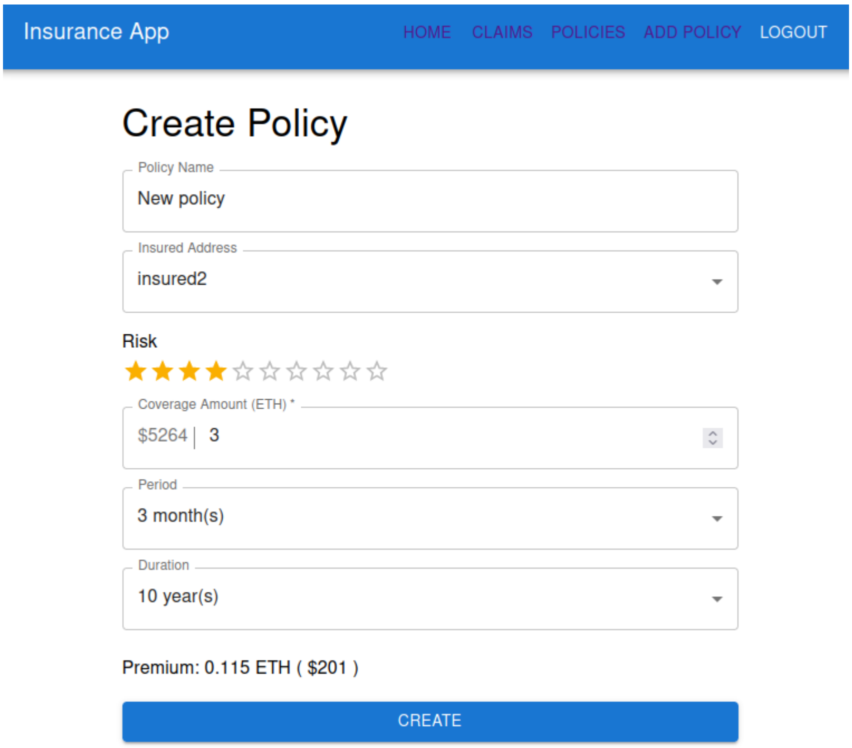

Figure 3.7: Create Policy

Policy creation in our system is a detailed and tailored process, designed to create a policy that is highly customizable and caters to the individual needs of each insured party. This process is initiated by the insurer who has the privilege of crafting new policies.

When an insurer decides to create a policy, they start by providing essential information such as a unique policy name and a comprehensive description. These help to clarify the purpose and coverage of the policy for potential insured parties.

The insurer also selects the name of the intended insured party from a dropdown menu. This feature ensures that each policy is created with a specific insured party in mind, thus making each policy a personalized and targeted product.

The next step involves the insurer assessing the risk associated with the insured. This is a crucial aspect that isn't directly stored within the system but significantly influences the terms of the policy. For instance, if the policy is a life insurance policy for a 90-year-old person, the assessed risk would be relatively high.

The insurer also sets the policy duration and premium frequency during the creation process. The duration can be 1 year, 2 years, 5 years, 10 years, 20 years, or 30 years, while the premium frequency can be set to every 30 days, 90 days, 180 days, or once a year. These options offer a level of flexibility, allowing the insurer to design a policy that suits the risk profile and financial capabilities of the insured.

The computation of the premium value is a crucial part of policy creation, and it involves a function that accounts for multiple variables: the coverage amount, the policy duration, the premium payment frequency, and the insured's risk level. This approach ensures that the premium is fairly calculated, reflecting the risk and commitment undertaken by both the insurer and the insured.

Upon completion of the policy creation process, the policy is registered in the blockchain, where it remains immutable and transparent. The named insured party then receives a request to accept the newly created policy, marking the beginning of its lifecycle.

Overall, the policy creation process is a comprehensive and detailed procedure that allows the insurer to craft a policy that best fits the needs of the insured while also accurately reflecting the risks involved.

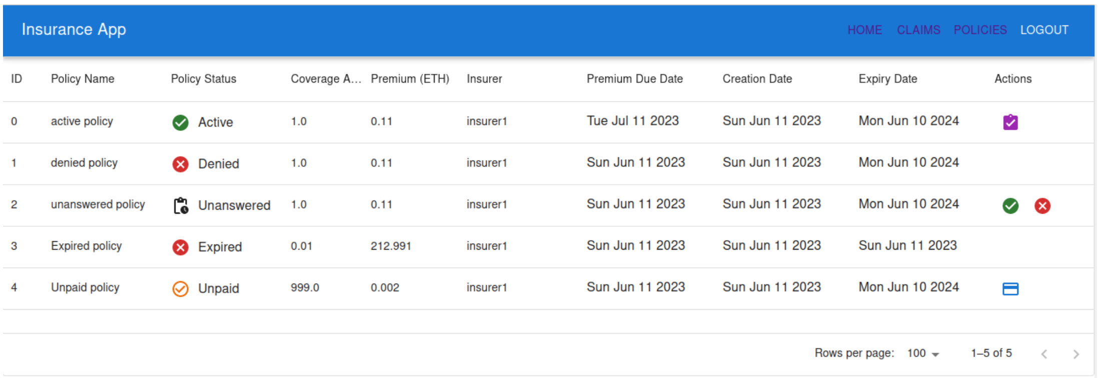

Figure 3.8: Policy table

Once a policy is created, the insured receives a policy request. If they accept the request, they make an initial premium payment, and the policy becomes active. If they deny the request, the policy remains in the system with a denied status.

An active policy can transition to an 'unpaid' status if the premium due date passes without payment. It can also expire naturally when its duration ends. Premiums can only be paid if the policy is in the 'unpaid' status.

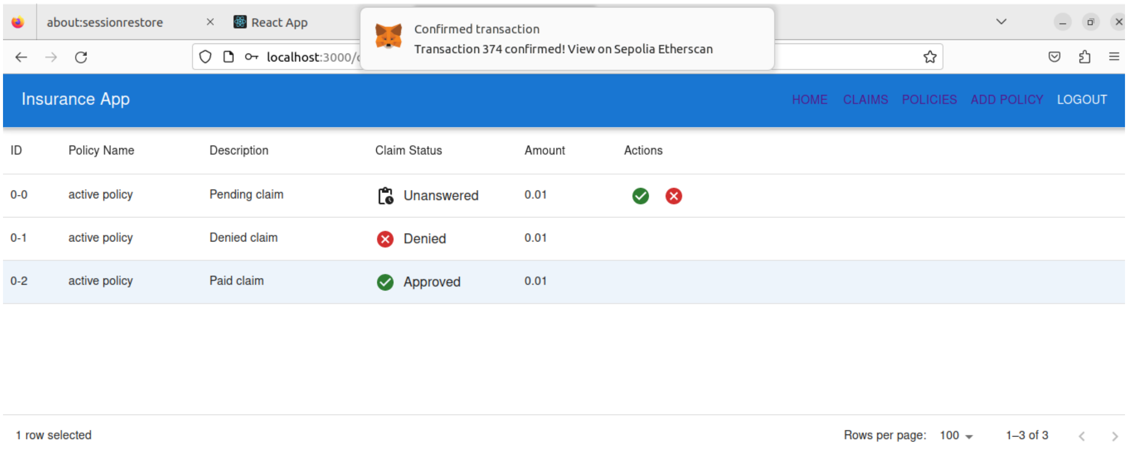

Figure 3.9: Claims table

Claims can be filed by the insured on active policies, specifying the claim description and the amount requested. These claims then appear in the insurer's claims table, and they can choose to accept or deny them. Acceptance of a claim triggers a transfer of the claim amount from the insurer to the insured.

To ensure fairness and prevent abuse, the system imposes limits on claims. The insured cannot claim an amount greater than the remaining policy coverage amount. If they attempt to claim a larger amount or make multiple claims that exceed the coverage amount, the smart contract rejects the transaction.

In this way, our system provides a robust and comprehensive platform for managing insurance policies and claims. It mirrors real-world insurance systems while benefiting from the transparency, immutability, and efficiency of blockchain technology.

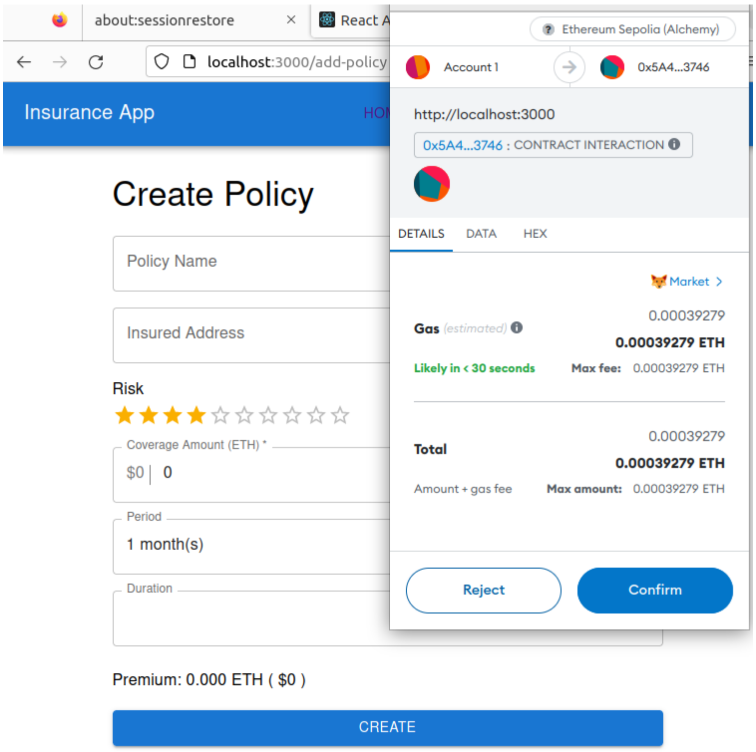

Figure 3.10: Metamask approval

Interacting with the smart contract in our system involves the use of MetaMask, a popular Ethereum wallet that integrates seamlessly with modern web browsers. Every significant operation, be it creating policies, filing claims, paying premiums, accepting policies, or settling claims, requires explicit confirmation through MetaMask. This confirmation step ensures that users are fully aware of the operations they're performing, adding an extra layer of security and control.

Each interaction with the smart contract incurs a small transaction fee, often referred to as "gas" in the Ethereum ecosystem. This fee compensates for the computational energy required to execute the operation on the blockchain. The fee amount is displayed in the MetaMask confirmation popup, giving users full transparency about the costs involved.

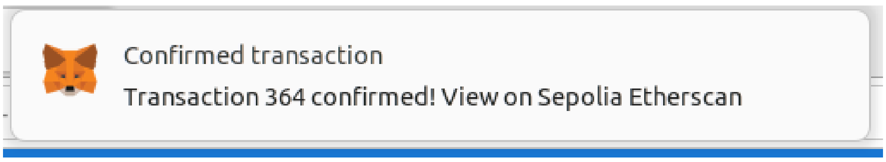

Figure 3.11: Transaction confirmation

After a user confirms an operation, the corresponding smart contract method is called. Upon the completion of the operation, a notification popup appears at the top of the page to inform the user of the operation's success.

It's important to note that using a decentralized system like this involves longer waiting times compared to traditional web applications. This is because we interact directly with the smart contract on the Ethereum network, and operations need to be validated and added to the blockchain. While this might take longer, it provides the unparalleled advantages of transparency, immutability, and security that are inherent to blockchain systems.

So while the waiting times might be slightly longer than what users are accustomed to in traditional applications, the benefits offered by our blockchain-based system – transparency, security, and a trustless environment – more than compensate for it.

Chapter 4

Evaluation

4.1 State of the Art

The application of blockchain technology in the insurance industry has seen substantial interest but remains largely uncharted. Zhou [Zho19] conducted a study wherein they proposed a method to enhance insurance claim management using blockchain technology. Their work demonstrated blockchain's potential to create a more efficient and transparent claim process. However, their research did not delve into a crucial area that blockchain could significantly impact - cost efficiency.

In another study, Kumar and Zeadally [KZ21] presented a blockchain-based framework for the insurance industry. Their approach highlighted the decentralization, transparency, and security benefits of blockchain. While their work provided a comprehensive framework for blockchain application, it did not directly address the nuances and specific requirements of risk management, a critical component of the insurance process.

Our research aims to explore these uncharted territories - the use of blockchain technology for robust cost efficiency, precise risk management, and improved transaction times in the insurance industry.

4.2 Approach

Our study is set against the backdrop of two major challenges in the insurance industry - high operational costs and inefficient risk management. We propose a theoretical model that integrates blockchain technology into the heart of the insurance process, specifically targeting cost efficiency and risk management.

The model is designed to leverage the inherent attributes of blockchain technology. Blockchain's immutability prevents tampering with historical data, making cost calculations more accurate. Its transparency ensures all parties have access to the same data, creating a single version of the truth and reducing disputes. This could be instrumental in improving trust and efficiency in the insurance process.

4.2.1 Qualitative analysis

The qualitative analysis was conducted by examining existing literature, case studies, and real-world applications of blockchain in the insurance industry. This approach aimed to understand the theoretical implications and practical applications of blockchain technology on risk management.

One of the standout attributes of blockchain technology is its inherent safety and security. The application of blockchain technology in the insurance industry can greatly enhance the security and reliability of the system, creating a safer environment for all stakeholders.

Our theoretical model, in line with the principles of decentralization and customization inherent in blockchain technology, allows for more personalized risk assessment and management. This is achieved by integrating risk as a determining factor when calculating the premium for an insurance policy.

In the policy creation component of our model, the premium is computed based on several variables: risk level, policy duration, coverage amount, and premium payment frequency. This approach facilitates a customized policy, wherein the premium varies directly with the level of risk. This means higher premiums for higher risks and lower premiums for lower risks, ensuring a proportionate and fair allocation of costs.

Risk (stars)	**Coverage Amount ($)**	**Period (days)**	**Duration (years)**	**Premium ($)**	**Total Paid ($)**
2	16568	30	1	1756	21072
5	16568	30	1	1849	22188
10	16568	30	1	1919	23028
2	16568	30	10	210	25200
5	16568	30	10	220	26400
10	16568	30	10	230	27600
10	16568	180	10	1320	26400

Table 4.1: Policy Premium and Total Paid based on Risk, Coverage Amount, Period, and Duration

This approach stands in contrast to traditional insurance companies, which often have standardized premium rates that do not sufficiently reflect individual risk levels. They generally use a one-size-fits-all model, which does not take into consideration the specific risks associated with each policyholder.

Hence, our blockchain model, with its personalized and risk-reflective premium calculation, offers a significant improvement in risk management efficiency. However, the flexibility of this approach will need to be further tested and validated in a real-world context to fully ascertain its practical implications and potential benefits.

Moreover, as part of future work, the inclusion of more variables and factors in the risk and premium calculation could be considered. This would allow for even more sophisticated and accurate risk assessment, thus enhancing the fairness and efficiency of the insurance process.

4.2.2 Quantitative Analysis

For the quantitative analysis, we focus on transaction cost and time. In terms of cost, we compare the total cost of operations in a 10-year insurance policy lifecycle using our blockchain-based model against that of traditional systems.

Table 4.2: Cost Efficiency Analysis

Operation	**Cost (ETH)**
Creation of Policy	0.004
Accepting of Policy	0.001
Filing Claim	0.003
Accepting Claim	0.001
Annual Premium Payment (10 years)	0.01
Total Cost	0.019

Regarding the transaction time, we measure the average time taken for various operations and compare it with the time taken by traditional insurance processes.

Table 4.3: Transaction Time Analysis

Operation	**Time (ms)**
Create Policy	22467
Accept Policy	27681
File Claim	23988
Accept Claim	24686
Pay Premium	25496

The performance of the blockchain-based model will be evaluated based on these quantitative comparisons. This will allow us to objectively assess the model's cost efficiency and speed.

4.3 Evaluation of the Approach

Our evaluation will involve both qualitative and quantitative analysis, using key performance metrics to assess the model's performance. Preliminary results indicate that the use of blockchain technology can significantly reduce operational costs and improve the efficiency of risk management, although it might slightly increase transaction times. However, it's crucial to note that while the transaction times may be longer, these transactions are completed in real-time, contrasting to traditional bank transactions that can take several days or even weeks to settle.

We determined the cost of policy creation, policy acceptance, claim filing, claim acceptance, and premium payment in the blockchain model, resulting in a total cost of 0.019 ETH for a 10-year insurance policy. Compared to the percentage fees often charged by traditional insurance companies using banking systems, the fixed cost of the blockchain model can be substantially lower, especially for higher-value policies.

It's also important to note that the transaction times recorded, despite being higher than typical web application response times, represent the real, completed transaction times. In contrast, traditional banking systems, though they might appear quicker, often 'hold' transactions, taking substantial time to complete the process.

However, further experimentation and a more extensive dataset are required to validate these results fully and draw robust conclusions. Therefore, we suggest future work include more diverse scenarios and larger datasets to assess the model's scalability and performance under different conditions.

Chapter 5

Conclusion

The integration of blockchain technology into the insurance industry holds tremendous promise for overcoming some of the sector's most pressing challenges. As demonstrated throughout this research, blockchain's unique attributes - decentralization, transparency, security, and immutability - could serve as key drivers for the significant enhancement of the insurance process.

From an operational perspective, blockchain can introduce a new level of efficiency and cost reduction. By harnessing the technology's immutability and transparency, we could create a more reliable and tamper-proof system for maintaining and accessing insurance data. This could eliminate costly disputes and promote trust amongst all parties involved.

The research conducted by Zhou [Zho19] and Kumar and Zeadally [KZ21] established the potential of blockchain for enhancing the insurance claim process and providing a decentralized and secure framework, respectively. However, these studies did not fully explore the technology's potential for cost efficiency and risk management.

Our research filled these gaps by proposing a blockchain-based model specifically designed to improve cost efficiency and precise risk management in the insurance industry. We incorporated risk as a determining factor in the calculation of insurance premiums, which facilitated a more personalized and fair allocation of costs. This model also enables faster transactions and a reduction in operational costs compared to traditional systems, potentially leading to significant savings over time.

Our qualitative and quantitative evaluations suggested that the blockchain-based model could indeed be beneficial. However, these findings are preliminary and based on theoretical assumptions and models. Further research, experimentation, and validation with a more extensive dataset in real-world scenarios are required to fully assess the potential benefits and possible limitations of our approach.

5.1 Future Work

Future work in this field could focus on the integration of advanced machine learning and artificial intelligence algorithms for automatic claim validation and claim payments. Machine learning algorithms could analyze the vast amount of data recorded on the blockchain to detect patterns, irregularities, and potential fraud. This automation could significantly improve the speed and accuracy of the claim validation process.

AI technology could further enhance this process by learning from previous claim records and automatically adjusting the claim validation process accordingly. The coupling of blockchain's transparency and immutability with the predictive capabilities of AI could result in a system where fraudulent claims are minimized, and valid claims are processed rapidly and accurately.

As the landscape of technology and finance continues to evolve, it's crucial for the insurance industry to embrace these advancements. The adoption of blockchain technology, as proposed in our research, could represent a significant step forward in this journey. The proposed future integration of AI and machine learning technologies could further revolutionize the industry, leading to a more automated, efficient, and secure insurance process. While the path is not without its challenges, the potential rewards in terms of cost savings, improved efficiency, and better risk management make this a pursuit worth undertaking.

Bibliography

[But14] Vitalik Buterin. A next-generation smart contract and decentralized application platform. 2014.

[CDE+16] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, Dawn Song, and Roger Wattenhofer. On scaling decentralized blockchains. *Financial Cryptography and Data Security*, pages 106–125, 2016.

[Coi21] Cointelegraph. What are smart contracts? a beginner's guide to automated agreements, 2021. Accessed: 2023-05-01.

[eth23] Etherisc, 2023. `https://etherisc.com/`.

[fiz23] Fizzy axa, 2023. `https://fizzy.axa/`.

[Fou22] Web3 Foundation. What is web 3.0?, 2022.

[GM19] Andr'es Guadamuz and Chris Marsden. Blockchain regulation. *European Data Protection Law Review*, 5(2):145–155, 2019.

[HHSBL08] James Hendler, Wendy Hall, Nigel Shadbolt, and Tim Berners-Lee. Web 3.0 emerging. *Computer*, 41(1):76–78, 2008.

[ins23] Insurwave, 2023. `https://insurwave.com/`.

[KZ21] R. Kumar and S. Zeadally. Blockchain framework for the insurance industry. *Journal of Information Systems and Technology Management*, 2021.

[Mou16] William Mougayar. *The business blockchain: promise, practice, and application of the next internet technology*. John Wiley & Sons, 2016.

[NBF+16] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

[TS18] Stefan Thomas and Evan Schwartz. Interledger: Creating a standard for open payments. *IEEE Internet Computing*, 22(2):29–36, 2018.

[TT16] Don Tapscott and Alex Tapscott. *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin, 2016.

[Vis21] Visa. Consensus mechanisms: How do they work?, 2021. Accessed: 2023-05-01.

[Woo19] Gavin Wood. Polkadot: Vision for a heterogeneous multi-chain framework. *White Paper*, 2019.

[Zho19] et al. Zhou. Improving insurance claim management using blockchain technology. *Journal of Insurance and Blockchain*, 2019.

[Zoh15] Aviv Zohar. Secure high-rate transaction processing in bitcoin. *Financial Cryptography and Data Security*, pages 507–527, 2015.

List of Figures