DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING,

SHARDA SCHOOL OF ENGINEERING AND TECHNOLOGY,
SHARDA UNIVERSITY, GREATER NOIDA

Insurance Framework based on Blockchain and Smart Contract

A project submitted
in partial fulfillment of the requirements for the degree of
Bachelor of Technology in Computer Science and Engineering

by

Abhishek kumar Singh (2019006160)
Sahil Shivhare (2019004504)

Supervised by:
Dr. Nishant Gupta, Assistant Professor
Co-Supervisor’s Name (Tejeswe Khanna)

May, 2023

CERTIFICATE

This is to certify that the report entitled “Insurance Framework based on Blockchain and Smart Contract” submitted by Mr. Abhishek kumar Singh (2019006160), Mr. Sahil Shivhare (190101257) to Sharda University, towards the fulfillment of requirements of the degree of Bachelor of Technology is record of bonafide final year Project work carried out by him/her in the Department of Computer Science and Engineering, School of Engineering and Technology, Sharda University. The results/findings contained in this Project have not been submitted in part or full to any other University/Institute for award of any other Degree/Diploma.

Signature of Supervisor

Name:

Designation:

Signature of Head of Department

Name:

(Office seal)

Place:

Date:

Signature of External Examiner

Date:

ACKNOWLEDGEMENT

A major project is a golden opportunity for learning and self-development. We consider ourself very lucky and honored to have so many wonderful people lead us through in completion of this project.

First and foremost we would like to thank Dr. Nitin Rakesh, HOD, CSE who gave us an opportunity to undertake this project.

My grateful thanks to **Dr. Nishant Gupta** for his guidance in my project work. who in spite of being extraordinarily busy with academics, took time out to hear, guide and keep us on the correct path. We do not know where we would have been without his help.

CSE department monitored our progress and arranged all facilities to make life easier. We choose this moment to acknowledge their contribution gratefully.

Name and signature of Students

Abhishek kumar Singh (2019006160)

Sahil Shivhare (2019004504)

ABSTRACT

Processing insurance claims requires a variety of human-agent interactions, multi-domain entities, and data from several sources. As a result, this procedure is typically time-consuming and labor-intensive. Platforms for intelligent automation built on blockchain technology can greatly increase the speed and scope of claims processing. Insurance policy claiming and settling is a complex process. This settlement process is challenging because of a variety of issues, such as hidden requirements from accusations of fraud by the client or the insurance body. The insurance sector could be completely transformed by the use of blockchain technology and smart contracts. The entire insurance processes, from verification to claim settlement, can be carried out with improved security and increased transparency with the adoption of blockchain technology. This paper gives a framework based on blockchain smart contracts for insurance. If all the requirements are fulfilled at the event of a claim, the transaction takes place; if not, it is rejected. To develop smart contracts, a programming language called Solidity is employed. The system makes use of the consensus algorithm known as Proof of Authority (PoA) for the validation of each transaction.

This Project investigates the idea of securing insurance through blockchain and smart contracts. Blockchain technology provides a decentralized and tamper-proof ledger for managing insurance policies and claims, while smart contracts offer an automated and trustworthy way to execute the policy terms. The use of blockchain and smart contracts can increase transparency, reduce fraudulent activities, and enhance the speed and efficiency of the claims process. Moreover, this technology allows for the creation of innovative insurance products that were previously not feasible due to high administrative costs. However, the paper also discusses the challenges and limitations of implementing blockchain-based insurance, including regulatory hurdles, scalability, and interoperability.

The incorporation of blockchain and smart contracts in the insurance sector can offer improved security and transparency, reduced fraud, and increased efficiency. To achieve these benefits, several algorithms can be utilized, including cryptographic hashing algorithms, consensus algorithms, and encryption algorithms. Cryptographic hashing algorithms guarantee the integrity of data and prevent unauthorized access to information stored on the blockchain. Consensus algorithms ensure that transactions are validated correctly and that the blockchain remains secure and reliable. Encryption algorithms protect sensitive data and restrict access to authorized parties only. The amalgamation of these algorithms with blockchain and smart contracts has the potential to transform the insurance industry by introducing new insurance products and services. However, implementing these algorithms requires a cautious assessment of regulatory and legal frameworks, scalability, and interoperability.

LIST OF FIGURES

LIST OF TABLES

CONTENTS

CHAPTER 1: INTRODUCTION

1.1 PROBLEM STATEMENT:

Fraud in the insurance industry is a major concern for both the insurance company as well as for the client. The entire insurance industry is dependent upon the trust which both parties behold. In recent times many events have been observed in which either side are involved in any ill-practices by using the loopholes in the agreement to get out the arrangement, from companies not fulfilling their side of the deal and client fooling the companies to get false insurance claim, these is due to lack of technology involvement and transparent process.

The insurance industry has encountered significant challenges, including fraud, a lack of transparency, and inefficiencies in the claims process. These issues result in mistrust between insurers and policyholders, resulting in higher costs and reduced customer satisfaction. Traditional insurance systems typically involve complicated and time-consuming procedures for verifying claims, leading to higher administrative costs and delays in processing claims.

Additionally, centralized systems are vulnerable to cyber-attacks and data breaches, potentially resulting in sensitive data loss and financial damage. As a result, a secure, transparent, and efficient insurance system is necessary to provide prompt, accurate, and trustworthy insurance services to policyholders.

Blockchain and smart contract technology may address these challenges by providing a decentralized, tamper-proof, and automated system that ensures data integrity, reduces fraud, and increases efficiency. However, the adoption of this technology presents several challenges, including regulatory barriers, scalability concerns, and interoperability issues. Therefore, research is required to investigate the use of blockchain and smart contracts in insurance and develop solutions to overcome these obstacles and provide secure and dependable insurance services.

1.2 PROJECT OVERVIEW:

Insurance processes are based on different levels of transaction between both parties (Client and Insurance company) in the process of insurance claim. As we have described the problem above, these usually occur during the process of transaction as it mainly consists of a human validator which leads to fraud, and companies internal processes are very complex for an outsider to understand, that make the client unaware of the current status of his claim. We proposed a solution which involves using smart contracts for the purpose of transaction in the insurance using Ethereum smart contract network.

Each transaction is done after it is verified by the validator using a consensus algorithm which works on Proof of Authority which has defined requirements when completed and verified transaction block and created , added to the private ethereum network. Consensus algorithm has a different set of algorithms each with its own functionality.

Which together make a framework for transaction in insurances. The primary objective of this project is to create a framework for secured insurance through blockchain and smart contracts. The goal is to explore the potential advantages of utilizing blockchain and smart contracts in the insurance industry, such as increased transparency, enhanced security, reduced fraud, and improved efficiency.

The project will start with a comprehensive review of the existing literature on blockchain technology and smart contracts, as well as their applications in the insurance sector. Additionally, the project will analyze various blockchain-based insurance use cases, including parametric insurance, peer-to-peer insurance, and microinsurance.

Next, the project will develop a framework for secured insurance through blockchain and smart contracts, emphasizing a decentralized, tamper-proof, and automated insurance system that ensures data integrity, reduces fraud, and enhances efficiency.

The framework will use various algorithms, including cryptographic hashing algorithms, consensus algorithms, and encryption algorithms, to guarantee the security and reliability of the insurance system. The final stage of the project will focus on implementing the framework to evaluate its feasibility and effectiveness.

The implementation will involve creating a proof-of-concept blockchain-based insurance system that demonstrates the essential features of the framework. The project will also identify and address the limitations and challenges of adopting blockchain-based insurance, including regulatory obstacles, scalability, and interoperability.

The project's findings will contribute to the development of a secure and efficient insurance system that provides reliable insurance services to policyholders while safeguarding data privacy and security.

1.3 **EXPECTED OUTCOME:**

The expected Outcome is a research-based output in which we will provide the framework that provides secured insurance through smart contract and blockchain.

The primary objective of this project is to develop a secured framework for insurance through blockchain and smart contracts, which aims to provide significant benefits to the insurance industry, such as enhanced security, transparency, reduced fraud, and increased efficiency. The project's expected outcomes are as follows:

1. Development of a comprehensive framework for secured insurance through blockchain and smart contracts that ensures data integrity, reduces fraud, and enhances efficiency.
2. Identification and addressing of the challenges and limitations of adopting blockchain-based insurance, including regulatory hurdles, scalability, and interoperability.
3. Creation of a proof-of-concept blockchain-based insurance system that demonstrates the key features of the framework, such as the decentralized, tamper-proof, and automated insurance system.

4. Validation of the feasibility and effectiveness of the framework by conducting thorough testing and evaluation.

Contribution to the development of a secure and efficient insurance system that provides trustworthy insurance services to policyholders while ensuring data security and privacy. The project will begin with a comprehensive review of the existing literature on blockchain technology and smart contracts and their applications in the insurance industry. Next, the project will focus on developing a framework for secured insurance through blockchain and smart contracts, using various algorithms to ensure the security and reliability of the insurance system.

The project will also address the challenges and limitations of adopting blockchain-based insurance, which may include regulatory barriers, scalability, and interoperability issues.The final stage of the project will focus on creating a proof-of-concept blockchain-based insurance system to test the feasibility and effectiveness of the framework.The expected outcome is a secured insurance framework that provides insurers with an innovative approach to improve their operations and customers with reliable and secure insurance services.

1.4 **HARDWARE & SOFTWARE SPECIFICATIONS:**

- At least 1gb ram (recommended 4gb).
- i5 processor or above.
- Operating System: Mac os, Windows, Linux
- Google Chrome, Firefox, Safari.
- Ethereum, Solidity.
- Development tools, including a code editor, a compiler, and a debugger. (Visual Studio Code)/MetaMask for token management.
- Web development frameworks, such as React or Angular, for building user interfaces
- Databases, such as MySQL or MongoDB, for storing and managing data
- Security tools, such as SSL certificates and encryption algorithms, to ensure data security and privacy.

In addition to the above hardware and software specifications, it is essential to have a team of developers with experience in blockchain, smart contracts, and insurance industry expertise. The team should be familiar with programming languages, such as Solidity, JavaScript, and Go, and have knowledge of blockchain-related technologies, including consensus algorithms, cryptography, and distributed ledger technology.

By adhering to these hardware and software specifications and having a skilled development team, an insurance framework based on blockchain and smart contracts can be created to provide secure, transparent, and efficient insurance services to policyholders.

1.5 **OTHER NON-FUNCTIONAL REQUIREMENTS:**

- High Storage space.
- Good Network Connectivity
- A reliable backup system for data recovery.

CHAPTER 2: LITERATURE SURVEY

2.1 EXISTING WORK:

S.no	Year/Author	Title	Contribution	Methods	Draw-backs	Conclusion
1.	2016/Hiroki Watanabe , Shigeru Fujimura	Blockchain Contract: Securing a blockchain applied to smart contracts.	For the security of a blockchain used for managing contracts, such as digital rights management, a new mechanism is suggested.	Deterrence by collapse of credibility.	Scalability energy consumption.	We have put forth a fresh method of safeguarding a blockchain used for managing contracts.
2.	2016, Sachchidanad singh.	Blockchain future of financial and cyber security.	This paper describes the idea, the traits, the necessity, and the operation of blockchain.	Authentication , integrity, Non-Repudiation.	Storage, Time-consuming.	A trustless system with peer-to-peer communications protocols and secure distributed data exchange can be provided via blockchain.
3.	2018, Mayank Raikwar, Subhra Mazumdar	A blockchain Framework for Insurance Processes.	To support transaction execution in insurance processes, create a distributed platform that uses blockchain as a system service.	Consensus algorithms.	Regulations, scalability.	The architecture for implementing transaction processes as smart contracts is proposed in this study and is based on the blockchain.
4.	2022, Saroj Kumar Nanda, Sandeep kumar Panda	Automating Vehicle insurance processing using smart Contract and Ethereum	Proposed a framework to avoid challenges like frauds, absence of P2P insurance, no timely settlement	Ethereum smart contracts	Legal formalities, Storage	Proposed framework for authentication of users and each step of insurance to be used.
5.	Ankitha Shetty	Blockchain Application in Insurance Services: A Systematic Review of the Evidence	This paper describes the idea, traits, and use of blockchain in insurance.	Authentication , Non-Repudiation.	Time Consuming.	Blockchain can protect us from fraudulent and offer a trustless system.

6.	Fahim Ullah Fadi Al-Turjman	A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities	Smart cities can implement blockchain smart contracts, and this article suggests a conceptual framework for doing so.	Ethereum Smart Contract	latency, size and bandwidth, wastage, limited usability, hard forks, multiple chains,	Using Google Trends, I listed the resources needed to implement this technology and the cities where it might be used.
7.	Jaideep gera	Blockchain Technology for Fraudulent Practices in Insurance Claim Process	With the help of this technology, every transaction is kept as a block in the distributed ledger that multiple people connected to the application may programmatically verify.	Algorithm: Insurance Claim Processing (ICP)	Scalability	It is suggested to use a framework to incorporate blockchain in insurance applications.

2.2 PROPOSED SYSTEM:

This proposed framework smears the technique to make a reasonable building involving smart contract and blockchain to bids. Its main objective is to leverage smart contracts and blockchain technology to assure safe, secure, and fraud-free transactions. By using blockchain to handle client entry, policy issuance, and settlement, this framework strengthens the overall protection framework. Each block in a blockchain is made up of data. Each block contains the exchange data, timestamp, and cryptographic key for the previous block. This innovation has been widely used for a variety of purposes. Since the introduction of Bitcoin in 2009 while highlighting the blockchain architecture, Blockchains have distinguished themselves with a variation of applications across a variety of sectors. The widespread use of Bitcoin transactions has been the most well-known implementation of blockchain technology to date. The major financial and banking industry [8] and the public authority's public administrations have been identified as two crucial areas where the appropriate implementation of blockchain innovation can lead to enhanced efficiency.

A few distinctive qualities of the blockchain technology make it ideal for applications involving money exchange. The decentralized, agreement, provenance, unchanging nature, and irrevocability characteristics of the blockchain are its core characteristics. Decentralized refers to the idea that no single entity with the greatest authority controls the entire blockchain, and it is an important aspect of the blockchain. The foundation of the entire structure is provided by the participants' common knowledge. We refer to this common understanding as agreement. This accord is what we mean when we talk about consensus. Once more, agreement is a vital feature of the blockchain. A blockchain network's participants can only conduct an exchange once they have reached consensus on it.

A proposed system for insurance claim using smart contracts and blockchain technology could greatly benefit the insurance industry. The system could potentially streamline the claims process, reduce fraud, and increase transparency and security. The system would involve creating a blockchain network that includes all relevant stakeholders, including the insurance provider, policyholders, and third-party service providers. The system would use smart contracts to automate the claims process, from the time a claim is submitted to the time the payout is executed.

When a claim is filed, the smart contract would automatically verify the policy's terms and conditions, as well as the claimant's identity and the authenticity of any evidence submitted. The smart contract would then calculate the appropriate payout amount based on the policy terms and initiate the payout process. The use of blockchain technology would provide an immutable and transparent record-keeping system that could be accessed by all relevant stakeholders, increasing transparency and reducing the risk of fraud. Each transaction would be recorded on the blockchain, creating an unchangeable and tamper-proof record of the claims process.

The system would also allow for real-time monitoring and reporting of claims data, which could help insurance providers identify trends and patterns in claims and adjust their policies and pricing accordingly. To ensure the system is plague-free, appropriate security measures would need to be in place to prevent unauthorized access and ensure the system's integrity. These measures could include multi-factor authentication, encryption, and regular audits and testing of the system's security protocols.

Overall, a proposed system for insurance claims using smart contracts and blockchain technology has the potential to revolutionize the insurance industry by increasing efficiency, reducing fraud, and increasing transparency and security.

2.3 FEASIBILITY STUDY:

A policy serves as the representation of an insurance contract, which provides the policyholder with financial security or compensation for losses from an insurance provider. The Insurance Industry has a valuation over $500 billion. Health, commercial, and auto insurance contracts come in a variety of forms.

These industries are present in many different countries around the world, and governments in places like the EU, Japan, Canada, and the majority of South American nations have created public policies. Although insurance policies are frequently used, resolving claims is not always a straightforward process. Insurance companies frequently violate the terms and conditions of the contract in order to avoid paying the insured.

In Some cases, false calm by the customers is a problem for the Insurance entity.

Traditional agreement though legally binding can’t solve the above problems. These agreements are not straightforward and have escape clauses. These escape clauses lead to double-dealing generally speaking by the two safety net providers and customers. These issues can be resolved with blockchain-based smart contracts since they reduce the need for trust and financial burden in the present insurance process and offer precise clarity. The framework's primary objective is to leverage the power of smart contracts and blockchain technology to ensure that all transactions are safe, secure, and free of fraudulent activities.

By using blockchain to manage client access, policy issuance, and settlement, this framework strengthens the overall security infrastructure. Consensus is another critical aspect of the blockchain, which is the participants' agreement or common understanding. Participants in a blockchain network can only engage in transactions once they have reached a consensus on the transaction.

Insurance claims using blockchain and smart contracts are highly feasible and have the potential to revolutionize the insurance industry. Smart contracts are self-executing digital contracts that automatically execute when specific conditions are met. Blockchain technology, on the other hand, provides an immutable and transparent record-keeping system that can verify and validate transactions without the need for intermediaries.

In the insurance industry, blockchain technology can be used to store policy information, claims data, and transaction history securely and transparently. The use of smart contracts can automate the claims process by eliminating the need for intermediaries, reducing the time and cost associated with traditional claim processing.

When a claim is filed, the smart contract can automatically verify the policy's terms and conditions and initiate the claims process. The claimant can submit evidence of the claim, and the smart contract can automatically verify the authenticity of the evidence and calculate the appropriate payout amount based on the policy terms. Once the claim is validated, the smart contract can automatically execute the payout.

The use of blockchain and smart contracts for insurance claims can also reduce fraud by providing an immutable and transparent record of transactions. The technology can help prevent duplicate claims and identify fraudulent activities, reducing the risk for insurance providers.Overall, the feasibility of insurance claims using blockchain and smart contracts is high, and the technology has the potential to improve the speed, efficiency, and security of the claims process while reducing costs for both insurance providers and customers.

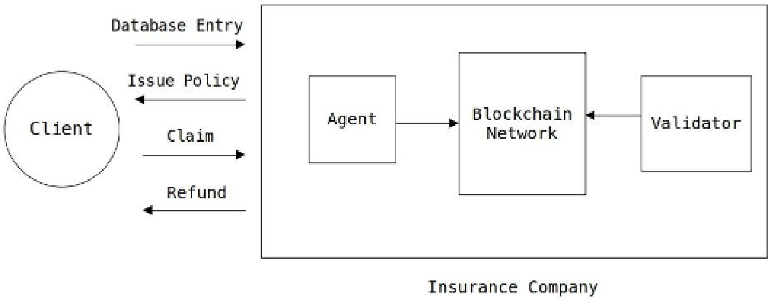


Fig 1: Diagram of Full System

CHAPTER 3: SYSTEM DESIGN & ANALYSIS

3.1 PROJECT PERSPECTIVE:

The design and analysis of a system for an insurance framework based on blockchain and smart contracts involve several stages. These stages include requirements gathering, system architecture design, database design, and user interface design. Below is an overview of the system design and analysis process for an insurance framework based on blockchain and smart contracts:

3.1.1 REQUIREMENTS GATHERING:

The first step is to gather the requirements for the insurance system. This process involves identifying the essential features of the system, such as policy creation, claims processing, and premium payment. It also involves identifying the stakeholders, such as policyholders, insurance providers, and regulatory authorities.

3.1.2 SYSTEM ARCHITECTURE DESIGN:

The next step is to design the system architecture for the insurance framework. This involves identifying the components of the system, including the blockchain network, smart contracts, and user interfaces. The system architecture should ensure security, scalability, and interoperability.

3.1.3 DATABASE DESIGN:

Database design is an essential aspect of the system design and analysis process. The database should store policyholder data securely, including policy details, claims history, and payment information. The design should also incorporate blockchain technology to ensure data integrity and immutability.

3.1.4 SMART CONTRACT DESIGN:

Smart contract design is a critical aspect of the system design and analysis process. The smart contract should automate insurance processes, such as policy creation, claims processing, and premium payment. The design should also incorporate business logic to ensure policy compliance and regulatory compliance.

3.1.5 USER INTERFACE DESIGN:

The user interface design is essential to the system design and analysis process. The user interface should provide an intuitive and user-friendly experience for policyholders, insurance providers, and regulatory authorities. The design should also incorporate blockchain technology to provide transparency and immutability.

3.1.6 TESTING AND DEPLOYMENT:

The final step is testing and deployment. The insurance framework should undergo thorough testing to ensure it meets the requirements and specifications. Once the testing is complete, the system can be deployed to production.

By following this process, an insurance framework based on blockchain and smart contracts can be designed to provide secure, transparent, and efficient insurance services to policyholders.

You see, blockchain technology is not just limited to bitcoin and other cryptocurrencies. It has a wide range of uses in various fields including insurance and health.The unique features of blockchain can benefit insurers in a number of ways, including cost savings, increased revenue, improved customer service, and more.

Blockchain has had transformational advantages for insurance firms.It's time for CTOs and CIOs in the insurance industry to realize blockchain's full potential and expand your business. Continue reading to learn how blockchain insurance claims, crypto-insurance, and other strategies may help you stay competitive in the market today.

The major Perspective of our research is that it will protect the consumer as well as the insurance company from the fraudulent activity involved in the process of insurance and establish trust between both the party and increase the transparency of the process of claim and settlement.

Blockchain has had a significant influence on such fraudulent scenarios in the insurance business. The way insurance firms conduct business might change because of technology.

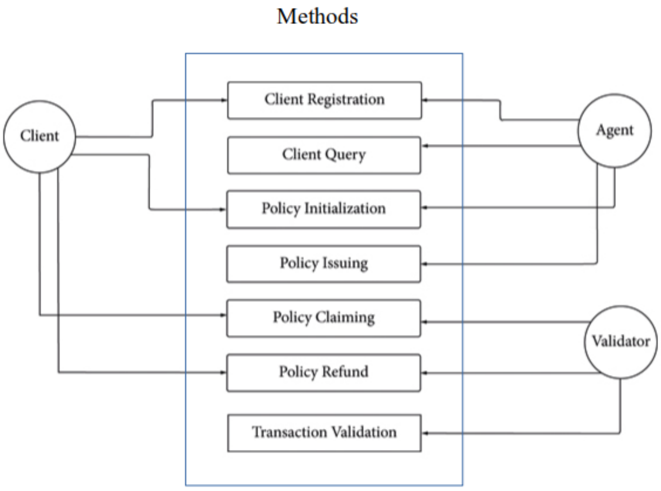


Fig 2: Low Level Design of the Framework

3.2 PERFORMANCE REQUIREMENTS:

- Require System with high computational power system.
- High Storage (Recommended using SSD).
- Good Network Connectivity (Internet).

Performance requirements are crucial to the successful implementation of an insurance framework based on blockchain and smart contracts. These requirements determine the system's capability to process a large volume of transactions, maintain data integrity, and ensure system availability. Below are some of the key performance requirements for an insurance framework based on blockchain and smart contracts:

3.2.1 TRANSACTION PROCESSING:

The insurance framework must be capable of processing a high volume of transactions efficiently. This capability is crucial to ensure timely policy creation, claims processing, and premium payment. The system should have a high throughput rate to handle the volume of transactions generated by policyholders, insurance providers, and regulatory authorities.

3.2.2 DATA INTEGRITY:

Ensuring the integrity of data stored in a blockchain network is crucial for a reliable insurance framework. To achieve this, it is necessary to utilize cryptographic algorithms to guarantee data security and prevent unauthorized access.

3.2.3 SYSTEM AVAILABILITY:

The insurance framework must ensure system availability at all times. The system should be designed to handle system failures and provide redundancy. The design should also incorporate load balancing techniques to ensure the system can handle high traffic volumes.

3.2.4 SCALABILITY:

The insurance framework must be scalable to handle increasing transaction volumes over time. The system should be designed to add new nodes to the blockchain network as the transaction volume increases. The design should also incorporate horizontal scaling techniques to ensure the system can handle multiple concurrent users.

3.2.5 RESPONSE TIME:

The insurance framework must have a fast response time to provide a seamless user experience. The system should have low latency to ensure that policyholders, insurance providers, and regulatory authorities can access the system quickly. The design should also incorporate caching techniques to reduce response time.

3.2.6 SECURITY:

The insurance framework must ensure system security. The system should use secure communication protocols, such as Transport Layer Security (TLS), to protect against network attacks. The design should also incorporate access control mechanisms to ensure that only authorized users can access the system.

By meeting these performance requirements, an insurance framework based on blockchain and smart contracts can provide efficient, secure, and reliable insurance services to policyholders.

3.3 SYSTEM FEATURES:

- High Security.
- Requires Less Time.
- Platform Independent.
- Low Cost.
- High Response Time.
- Each Activity can be monitored (Using logs).

A secure framework for insurance through blockchain and smart contract system features would consist of several elements to ensure transparency, security, and automation.

Firstly, a decentralized and immutable ledger would be used to store all insurance-related transactions, providing a secure and transparent record accessible to all parties involved.

Secondly, smart contracts would automate the insurance process from underwriting to claims management. These contracts would execute specific actions when certain conditions are met, such as paying out a claim when the loss event is verified.

To ensure that only eligible parties participate in the insurance scheme, Know Your Customer (KYC) and identity verification mechanisms would be in place. The blockchain-based system would use cryptographic security measures to protect the privacy and confidentiality of the data stored on the blockchain. Automated claims management would ensure that claims are processed quickly and accurately, and real-time monitoring would enable prompt detection of fraud or other issues. Tokenization of insurance policies and claims would enable easy transfer and trading of insurance products, enhancing liquidity and accessibility.

The blockchain-based system would allow for multi-party access to insurance policies and claims, ensuring that all parties have access to the same information, reducing the likelihood of disputes. Overall, a blockchain-based insurance system with smart contract features would provide a secure, transparent, and automated framework for insurance, offering significant benefits over traditional insurance systems.

3.4 METHODOLOGY:

The techniques and materials used to accomplish the objective are talked about in this segment. The objective is to make a protection biological system utilizing blockchain innovation. The main idea is to demonstrate the agreement's full capacity and execution. Its circumstances and justification for execution will be written using the Solidity programming language and organized as magnificent agreements. On an Ethereum-based distributed stage using blockchain technology, these negotiations will be managed. The main part of this section offers a simple framework model for the structure. The auxiliary resources present the pertinent features, the insurance structure's system, the network stage, agreement calculations, blockchain blocks, dazzling policies, and the structure's components and calculations. The findings and structure investigation are presented in segment three.

The execution of blockchain innovation in the sphere of numerous protection processes is the important commitment of this proposed framework. Additionally, it makes use of a specific agreement computation (for this situation: Proof of Authority) in the framework and the point-by-point calculation and the clarification of the entire cycle.

Blockchain networks employ consensus methods to achieve consensus across several distant nodes.By utilizing a consensus approach, such as proof of authority, to prevent unauthorized users from validating fraudulent transactions, network security can be established. Additionally, the technique permits network consensus even when no single node is in control. The framework generates and verifies transaction blocks before adding them to the Ethereum network using the Proof of Authority technique. The insurance company will pre-select the validators.

New blocks and transaction logs can only be generated by users who have shown their credibility in that role. Once selected, the validators are allowed to provide transaction logs and other monitoring tools.

Developing a secured framework for insurance using blockchain and smart contract technology requires a well-defined methodology. Here are the steps to be followed:

1. Define the requirements: The initial step is to define the requirements of the blockchain-based insurance system. This includes identifying the stakeholders, their roles, and the data that needs to be stored on the blockchain.

2. Choose the blockchain platform: Selecting a blockchain platform that meets the system requirements is essential. Factors to consider include the level of decentralization, transaction speed, and security.

3. Develop the smart contracts: Smart contracts automate the insurance process from underwriting to claims management. The rules for claims validation and processing, policy issuance, and premium payments need to be defined.

4. Implement KYC and identity verification: The system should implement KYC and identity verification mechanisms to ensure that only eligible parties participate in the insurance scheme.

5. Configure the blockchain network: The blockchain network needs to be configured once the smart contracts are developed and migration mechanisms are in place. This involves setting up nodes, choosing consensus mechanisms, and configuring the network for optimal performance.

6. Test and deploy the system: The system should be thoroughly tested before deployment to ensure that it meets the requirements and functions correctly. The deployment should be done in a controlled environment to ensure stability and security.

7. Monitor and maintain the system: Once deployed, the system must be monitored and maintained to ensure optimal performance. This includes performing regular security audits, updating the smart contracts, and upgrading the blockchain platform as necessary.

8. Continuously improve the system: The blockchain-based insurance system needs to be continuously improved to meet the changing needs of the stakeholders as the insurance market and regulatory environment evolve.

By following this methodology, a secured framework for insurance using blockchain and smart contract technology can be developed, meeting the requirements of the stakeholders and providing significant benefits over traditional insurance systems.

We have designed algorithms for each of the following functions:

- **CLIENT REGISTRATION**: Smart contracts can handle client registration in the blockchain-based insurance system. Clients can provide their details to the smart contract, which would verify their information against the KYC and identity verification mechanisms in place. Once validated, the smart contract would generate a unique identifier for the client and store their information on the blockchain in a tamper-proof and secure manner
  .
- **CLIENT QUERY**: Clients can query their insurance policy details by interacting with the smart contract. The smart contract would retrieve the client's policy details from the blockchain and provide them to the client in a transparent and secure way. This eliminates the need for intermediaries and reduces the risk of errors or fraud.

- **POLICY INITIALIZATION**: Smart contracts can automate policy initialization. When a client applies for insurance, the smart contract would assess the risk associated with the policy and validate the policy details. If the policy is approved, the smart contract would generate a unique identifier for the policy and store the policy details on the blockchain in a transparent and secure way.

- **POLICY ISSUING**: Smart contracts can also automate policy issuance. When a policy is approved, the smart contract would issue the policy to the client by storing the policy details on the blockchain. The policy details would be transparent and accessible to authorized parties on the blockchain network.

- **POLICY CLAIMING**: Smart contracts can automate the claims process. When a client initiates a claim, the smart contract would verify the claim against the policy details stored on the blockchain. If the claim is valid, the smart contract would automatically process the claim and release the funds to the client's account in a secure, transparent, and tamper-proof manner.

- **POLICY REFUND**: Smart contracts can also handle policy refunds. The smart contract would follow predefined refund rules and process the refund automatically. The refund would be transparent and visible to authorized parties on the blockchain network in a tamper-proof and secure manner.

By implementing these functions using blockchain and smart contract technology, the insurance process becomes more secure, efficient, and transparent. The decentralized nature of the blockchain ensures that the data is secure, while smart contracts automate the insurance process, reducing the risk of errors and fraud.

3.5 SMART CONTRACT IN USE:

A smart contract is a computer program that executes the terms of a contract automatically when specific predefined conditions are fulfilled. These contracts are usually built using blockchain technology, which offers a decentralized and secure way to store and manage data.Smart contracts provide an efficient and secure method for parties to conduct transactions without the need for intermediaries. By utilizing blockchain technology, smart contracts ensure transparency and tamper-proof execution of the terms of the agreement.

When it comes to insurance claims, smart contracts can be used to automate the claims process, reducing the time and cost associated with manual claims processing. Here's an example of how a smart contract for insurance claims might be structured:

- **DEFINING TERMS:** The smart contract would start by defining the terms of the insurance policy, including the coverage limits, deductibles, and exclusions.

- **VERIFICATION OF POLICYHOLDER INFORMATION:** The smart contract would then verify the identity of the policyholder and confirm that they meet the conditions of the policy.

- **TRIGGERING THE CLAIMS PROCESS:** Once a claim is submitted, the smart contract would automatically trigger the claims process, verifying the details of the claim against the terms of the policy.

- **VERIFICATION OF CLAIMS INFORMATION:** The smart contract would then verify the details of the claim, including the cause of the loss, the date and time of the loss, and any other relevant information.

- **CALCULATION OF PAYOUT:** Based on the information verified in step 4, the smart contract would calculate the payout amount according to the terms of the policy.

- **TRANSFER OF FUNDS:** Finally, the smart contract would automatically transfer the payout amount to the policyholder's account.

By using a smart contract for insurance claims, insurers can reduce the risk of fraud and errors, while policyholders can enjoy a faster and more efficient claims process. Additionally, since the smart contract is executed automatically, there is no need for intermediaries or manual processing, which can reduce costs and increase transparency.

1. **POLICY CREATION:** The first step in creating a smart contract for insurance claims is to define the terms of the policy. This includes the coverage limits, deductibles, and any exclusions or conditions that must be met for a claim to be valid.

2. **POLICY VERIFICATION**: Once the policy is created, the smart contract can automatically verify the policyholder's information and ensure that they meet the requirements of the policy.

3. **CLAIM SUBMISSION**: When a claim is submitted, the smart contract will automatically trigger the claims process. This can include verifying the details of the claim, such as the cause of the loss and the amount being claimed.

4. **VERIFICATION OF CLAIMS INFORMATION**: The smart contract will then verify the details of the claim against the terms of the policy. This can include verifying the date and time of the loss, as well as any other relevant information.

5. **CALCULATION OF PAYOUT**: Based on the verified details of the claim, the smart contract will calculate the payout amount according to the terms of the policy.

6. **TRANSFER OF FUNDS**: Finally, the smart contract will automatically transfer the payout amount to the policyholder's account.

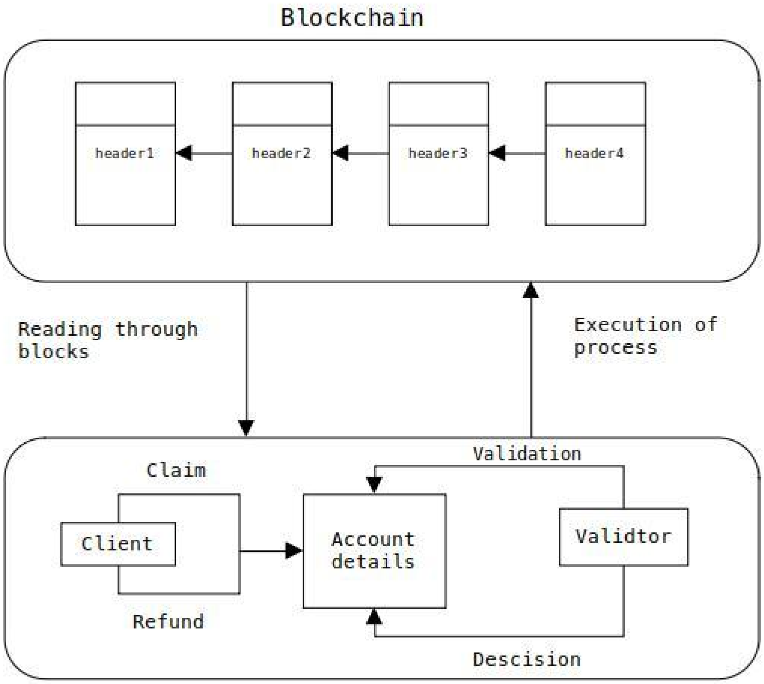


Fig 3: The Structure of the Smart contract

Auth Sol:

The Entire Smart contract that deals with the consensus on both sides of the party involved..

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract Auth {
  uint public insuranceId=0;
  uint public nextId=0;

  struct Insurance{
    uint id;
    address insuredBy;
    address doctor;
    string reason;
    bool isApproved;
    uint amount;
  }
  event InsuranceCreated(
     uint id,
    address insuredBy,
    address doctor,
    string reason,
    bool isApproved,
    uint amount
  );

  struct UserDetail {
     address addr;
     address draddr;
     string name;
     string password;
     bool isUserLoggedIn;
    bool isDoctor;
    uint Amount;
  }
  mapping(address => UserDetail) user;
  address[] public doctorAccounts;

  Insurance[] public insurance;
  Insurance[] public userinsurance;
  uint[]  public userinsurances2;
  modifier checkIsUserLogged2 {
       require(user[msg.sender].isUserLoggedIn == true, "Action not permitted user need to login first");
    _;
  }
  function totaldoctorInsurance(address _addr )external view returns(uint) {
    uint count=0;
    for (uint i = 0; i < insurance.length; i++) {
      if(insurance[i].doctor==_addr){
        count++;
      }
    }
    return count;
  }
  function totaluserInsurance(address _addr )external view returns(uint) {
    uint count=0;
    for (uint i = 0; i < insurance.length; i++) {
      if(insurance[i].insuredBy==_addr){
        count++;
      }
    }
    return count;
  }
   function getUserInsurance(address _addr )view external returns(uint,string memory,string memory,string memory,uint,address ) {
        string memory reason1="hello";
        string memory isApproved1;
        string memory drname1;
        address temp;
        uint amount1;
        uint id1;

        for (uint i = 0; i < insurance.length; i++) {
           if(insurance[i].insuredBy==_addr){
              reason1 = insurance[i].reason;
                        id1 = insurance[i].id;

              amount1 = insurance[i].amount;
              temp = insurance[i].doctor;
              drname1 = getDoctor(temp);
              if(insurance[i].isApproved){
                 isApproved1="true";
              }else{
                 isApproved1="false";
              }
           }
        }
        return (id1,drname1,reason1,isApproved1,amount1,temp);
    }
       function getUserInsuranceById(uint id)view external returns(uint,string memory,string
memory,string memory,uint,address,address ) {
        string memory reason1="hello";
        string memory isApproved1;
        string memory drname1;
        address temp;
        address temp2;
        uint amount1;
        uint id1;
```

```
            reason1 = insurance[id].reason;
                        id1 = insurance[id].id;

            amount1 = insurance[id].amount;
            temp = insurance[id].doctor;
            temp2 = insurance[id].insuredBy;
            drname1 = getDoctor(temp);
            if(insurance[id].isApproved){
               isApproved1="true";
            }else{
               isApproved1="false";
            }


      return (id1,drname1,reason1,isApproved1,amount1,temp,temp2);
   }
      function getDoctorInsuranceForApproval(address _addr )view external returns(string
memory,string memory,string memory,uint,address ) {
      string memory reason1="hello";
      string memory isApproved1;
      string memory drname1;
      address temp;
      uint amount1;
      for (uint i = 0; i < insurance.length; i++) {
         if(insurance[i].doctor==_addr){
            reason1 = insurance[i].reason;
            amount1 = insurance[i].amount;
            temp = insurance[i].doctor;
            drname1 = getDoctor(temp);
            if(insurance[i].isApproved){
               isApproved1="true";
            }else{
```

```
          isApproved1="false";
        }
      }
    }
    return (drname1,reason1,isApproved1,amount1,temp);
  }
  function isDr(address _address) public view returns(bool){
    return (user[_address].isDoctor);
  }
  function getDoctors() view public returns (address[] memory) {
    return doctorAccounts;
  }
  function getDoctor(address _address) view public returns (string memory) {
    return (user[_address].name);
  }
  function countDoctors() view public returns (uint) {
    return doctorAccounts.length;
  }
   function createInsurance(address _insuredBy,string memory _reason,uint _amount) public
checkIsUserLogged2{
    address drtemp= user[_insuredBy].draddr;
    uint id2=insuranceId;
    insurance.push(Insurance(id2, _insuredBy, drtemp, _reason,false, _amount));
    emit InsuranceCreated(id2,_insuredBy, drtemp, _reason, false, _amount);
    insuranceId++;
  }
  function approveInsurance(uint id) public {
    uint id2=find(id);
    insurance[id2].isApproved=true;

  }
  function disapproveInsurance(uint id) public checkIsUserLogged2{
    uint id3=find(id);
    insurance[id3].isApproved=false;
```

```
}
function find(uint id) view internal returns(uint){
    for (uint i = 0; i < insurance.length; i++) {
        if(insurance[i].id==id){
            return i;
        }
    }
    revert('claim does not exists');
}

// user registration function
function register(
    address _address,
    address _draddress,


    string memory _name,
    string memory _password,


    bool _isDoctor
) public returns (bool) {
    require(user[_address].addr != msg.sender);
    user[_address].addr = _address;
    user[_address].draddr = _draddress;
    user[_address].name = _name;
    user[_address].password = _password;
    user[_address].isUserLoggedIn = false;
    user[_address].Amount = 1000;
    user[_address].isDoctor = _isDoctor;
    nextId++;
    if(_isDoctor==true){
    doctorAccounts.push(_address);
    }

    return true;
    }

    // user login function
    function login(address _address, string memory _password) public returns (uint){
        bytes memory b1 = bytes(_password);
        bytes memory b2 = bytes(user[_address].password);
        uint256 l1 = b1.length;
        if (l1 != b2.length){
            return 0;
        }
        for (uint256 i=0; i<l1; i++) {
            if (b1[i] != b2[i]) {
                return 0;
            }

        }
            user[_address].isUserLoggedIn = true;
            return 1;
    }

    // check the user logged In or not
    function checkIsUserLogged(address _address) public view returns (bool) {
        return (user[_address].isUserLoggedIn);
    }

    // logout the user
    function logout(address _address) public {
        user[_address].isUserLoggedIn = false;
    }
}
```

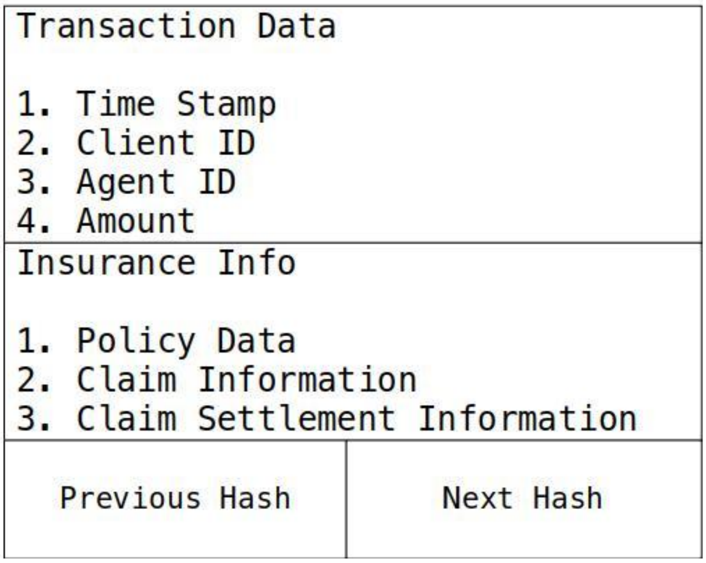
MIGRATION SOL:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract Migrations {
  address public owner = msg.sender;
  uint public last_completed_migration;

  modifier restricted() {
    require(
      msg.sender == owner,
      "This function is restricted to the contract's owner"
    );
    _;
  }

  function setCompleted(uint completed) public restricted {
    last_completed_migration = completed;
  }
}
```



Transaction Data

1. Time Stamp
2. Client ID
3. Agent ID
4. Amount

Insurance Info

1. Policy Data
2. Claim Information
3. Claim Settlement Information

Previous Hash

Next Hash

Fig 4: Detail of BlockChain Block

CHAPTER 4: DEVELOPMENT & IMPLEMENTATION

4.1 DEVELOPMENT FEASIBILITY

The developmental feasibility of a secured insurance framework using blockchain and smart contract technology is a topic of great interest among industry experts and researchers. While blockchain technology is considered revolutionary for its ability to create decentralized and secure systems, there are several factors to consider when developing a blockchain-based insurance framework.

One of the primary considerations for the developmental feasibility of a blockchain-based insurance framework is the existing technological infrastructure. Building a blockchain-based insurance framework requires a robust technological infrastructure, which includes a secure blockchain network, smart contract development tools, and API integration capabilities. It is important to evaluate the existing technological infrastructure to ensure that it can support the blockchain-based system. If the current infrastructure is not sufficient, the necessary upgrades and modifications must be made to accommodate the new system.

Another important factor to consider is the availability of skilled developers. Developing a blockchain-based insurance framework requires a team of skilled developers with expertise in blockchain development, smart contract programming, and insurance systems. These developers should also have knowledge of security protocols, encryption, and decentralization. Hiring a skilled development team with relevant experience can help to ensure the successful development of the blockchain-based insurance framework.

Regulatory compliance is also an important factor to consider when developing a blockchain-based insurance framework. The framework should comply with legal and regulatory frameworks in the jurisdiction it is deployed in. Regulatory compliance is critical to ensure that the blockchain-based insurance framework is legally valid and can be used in a commercial setting.

User adoption is another key consideration for the developmental feasibility of a blockchain-based insurance framework. The framework should be designed to be user-friendly and easy to understand. Users should also be educated on the benefits of the blockchain-based insurance framework, such as transparency, security, and efficiency. User adoption is essential for the success of the blockchain-based insurance framework and can be achieved through effective marketing and communication strategies.

Scalability is also an important factor to consider when developing a blockchain-based insurance framework. The framework should be designed to handle a large volume of transactions and data and should be able to scale as the user base grows. Scalability is critical to ensure that the blockchain-based insurance framework can support the needs of a growing user base and is a key factor in ensuring the long-term success of the framework.

In conclusion, the developmental feasibility of a secured insurance framework using blockchain and smart contract technology depends on several factors. These factors include the existing technological infrastructure, availability of skilled developers, regulatory compliance, user adoption, and scalability. By carefully considering these factors and taking steps to ensure that each one is addressed during development, it is possible to create a robust and secure blockchain-based insurance framework that provides benefits such as transparency, security, and efficiency.

4.2: IMPLEMENTATION SPECIFICATIONS

The implementation specification for a secured insurance framework using blockchain and smart contract technology involves the following steps:

1. Determine the business requirements: The first step is to identify the business requirements for the secured insurance framework. This includes determining the types of insurance policies to be offered, the target market, and the user experience.

2. Choose the blockchain platform: The next step is to select the blockchain platform that best suits the project's requirements. Ethereum is a popular choice due to its smart contract capabilities.

3. Design the architecture: The architecture of the secured insurance framework should be designed next. This includes creating the necessary smart contracts, designing the user interface, and integrating external APIs.

4. Develop and test the smart contracts: The smart contracts that govern the insurance policies should be developed and tested. This includes writing code and conducting extensive testing to ensure that the smart contracts function correctly.

5. Develop the user interface: The user interface is a crucial component of the secured insurance framework. It should be user-friendly and straightforward to use, with clear instructions on how to buy policies, file claims, and receive payouts.

6. Integrate external APIs: Third-party APIs can be integrated to provide additional functionality to the secured insurance framework. This includes integrating with payment gateways, identity verification services, and other third-party services required for the system's smooth operation.

7. Test the system: After the development of the secured insurance framework is complete, it should be thoroughly tested to ensure that it operates as expected. This includes testing the smart contracts, user interface, and external APIs.
8. Deploy the system: Once testing is complete, the system can be deployed on the chosen blockchain platform. This involves deploying the smart contracts and user interface to the blockchain network.

9. Monitor and maintain the system: The secured insurance framework should be monitored and maintained to ensure that it functions correctly after deployment. This includes monitoring the blockchain network for any issues, updating the smart contracts as required, and responding to any user inquiries or issues.

By following these steps, a secure and efficient insurance framework can be created using blockchain and smart contract technology, providing benefits such as transparency and security to users.

4.3: SYSTEM MODULES AND FLOW OF IMPLEMENTATIONS

4.3.1 SYSTEM MODULES:

The secured insurance framework using blockchain and smart contract technology can be divided into the following modules:

1. User Interface: This module provides the user interface for clients to interact with the system. It allows them to buy policies, file claims, and receive payouts.

2. Smart Contract Module: This module contains the smart contracts that govern the insurance policies. It includes functions for policy initialization, policy issuing, claiming, and refunding.

3. Payment Gateway Integration Module: This module integrates the payment gateway to allow clients to make premium payments for their policies.

4. Identity Verification Module: This module verifies the identity of clients to prevent fraud and ensure that only legitimate claims are made.

5. Insurance Pool Module: This module manages the insurance pool and distributes payouts to clients when claims are made.

4.3.2 FLOW OF IMPLEMENTATION:

The flow of implementation for a secured insurance framework using blockchain and smart contract technology can be summarized as follows:

1. Client Registration: Clients must register with the system and provide their personal information and payment details.

2. Policy Initialization: The client selects the insurance policy they wish to purchase and pays the premium using the integrated payment gateway.

3. Policy Issuing: Once the premium payment is confirmed, the smart contract issues the policy to the client.

4. Claiming: If the client experiences an event covered by the policy, they can file a claim. The identity verification module ensures that the claim is legitimate, and the smart contract initiates the payout from the insurance pool.

5. Refund: If the client cancels their policy before the coverage period ends, they may be eligible for a refund. The smart contract calculates the refund amount and initiates the refund to the client's account.

6. System Monitoring and Maintenance: The system must be monitored and maintained to ensure that it functions correctly. This includes monitoring the blockchain network for any issues, updating the smart contracts as required, and responding to any user inquiries or issues.

By following this flow of implementation and utilizing the system modules, a secured insurance framework using blockchain and smart contract technology can be developed and implemented. This framework provides benefits such as transparency, security, and efficiency to clients, ensuring a trustworthy insurance system.

4.4 CRITICAL MODULES OF PRODUCT/SYSTEM:

Here are the critical modules of a product/system for a secured insurance framework using blockchain and smart contract technology:

- **SMART CONTRACT MODULE:**
  The smart contract module is the backbone of the system. It includes functions for policy initialization, policy issuing, claiming, and refunding. Smart contracts are self-executing and operate autonomously on the blockchain network, allowing for transparency and security in the insurance process.

- **PAYMENT GATEWAY INTEGRATION MODULE:**
  The payment gateway integration module is crucial for the system, as it allows clients to pay their insurance premiums and receive payouts for claims. This module is responsible for integrating payment gateways and ensuring that payment transactions are secure and processed efficiently.

- **IDENTITY VERIFICATION MODULE:**
  The identity verification module is critical to prevent fraud and ensure that only legitimate claims are made. This module verifies the identity of clients using various identification methods, such as biometric verification, ID card verification, or facial recognition.

- **INSURANCE POOL MODULE:**
  The insurance pool module manages the funds collected from clients' premiums and distributes payouts to clients when claims are made. This module ensures that funds are secure and managed efficiently, allowing for timely payouts to clients.

- **USER INTERFACE MODULE:**
  The user interface module provides clients with an intuitive and easy-to-use interface to interact with the system. This module allows clients to view their policy details, file claims, and receive payouts. A user-friendly interface is critical to the success of the system, as it can encourage clients to use the system and increase user satisfaction.

- **BLOCKCHAIN NETWORK MODULE:**
  The blockchain network module is the foundation of the system. It provides the distributed ledger technology and cryptographic protocols required for the system's security, transparency, and immutability. The blockchain network module is responsible for managing transactions, storing data, and maintaining the system's integrity.

In conclusion, the critical modules of a product/system for a secured insurance framework using blockchain and smart contract technology are the smart contract module, payment gateway integration module, identity verification module, insurance pool module, user interface module, and blockchain network module. These modules work together to create a transparent, secure, and efficient insurance system that benefits both clients and insurers.

CHAPTER 5: RESULT / OUTPUT & TESTING

5.1: RESULT

- The result of our topic that is secured insurance framework using blockchain and smart contract technology, is a system that offers numerous benefits to clients and insurers alike. The implementation of such a system can revolutionize the insurance industry, making it more transparent, secure, and efficient.

- By utilizing blockchain technology, the system creates a distributed ledger that records every transaction and policy detail, allowing for transparency and immutability. Smart contracts enable automated policy issuance, claims processing, and refunding, eliminating the need for intermediaries and reducing the time and costs associated with insurance transactions.

- Additionally, the system's payment gateway integration module ensures that payment transactions are secure and processed efficiently, while the identity verification module prevents fraud and ensures that only legitimate claims are made. The insurance pool module manages the funds collected from clients' premiums and distributes payouts to clients when claims are made, ensuring that funds are secure and managed efficiently.

- The user interface module provides clients with an intuitive and easy-to-use interface to interact with the system, allowing clients to view their policy details, file claims, and receive payouts. Finally, the blockchain network module provides the distributed ledger technology and cryptographic protocols required for the system's security, transparency, and immutability.

- Overall, a secured insurance framework using blockchain and smart contract technology offers numerous benefits, including increased efficiency, security, transparency, and cost-effectiveness. The implementation of such a system can help streamline the insurance process, improve customer satisfaction, and reduce the risks and costs associated with insurance transactions.

5.2: OUTPUT

- In this paper we proposed a framework which smears the technique to make a reasonable building involving smart contract and blockchain to bids.
- Its main objective is to leverage smart contracts and blockchain technology to assure safe, secure, and fraud-free transactions. By using blockchain to handle client entry, policy issuance, and settlement, this framework strengthens the overall protection framework.
- We will provide a login portal that will enable the registration of the user and then can be implemented under the smart contract.
- A web based application.

5.3: TESTING

5.3.1: TYPE OF TESTING ADAPTED

1. **Unit Testing:**
   Unit testing involves testing each module of the system individually to ensure that it meets its specified requirements. For the smart contract module, this would involve testing functions such as policy initialization, policy issuing, claiming, and refunding. The payment gateway integration module can be tested by simulating payment transactions and ensuring that they are secure and processed efficiently. The identity verification module can be tested by verifying the identity of various users using different verification methods. The insurance pool module can be tested by simulating various scenarios, such as a large number of claims being made simultaneously, to ensure that funds are managed efficiently.

2. **Integration Testing:**
   Integration testing involves testing the interactions between different modules of the system to ensure that they work together seamlessly. For the insurance framework, this would involve testing the interactions between the smart contract module, payment gateway integration module, identity verification module, insurance pool module, user interface module, and blockchain network module. Integration testing can be done by simulating various scenarios, such as a client filing a claim and receiving a payout, to ensure that all modules work together efficiently.

3. **System Testing:**
   System testing involves testing the system as a whole to ensure that it meets the specified requirements. For the insurance framework, this would involve testing the entire system, including all modules and their interactions. System testing can be done by simulating various scenarios, such as a client registering for a policy, making payments, filing claims, and receiving payouts, to ensure that the entire process is efficient, secure, and transparent.

4. **Performance Testing:**
   Performance testing involves testing the system's performance under various loads to ensure that it can handle a large number of transactions without any performance issues. For the insurance framework, this would involve testing the system's performance under different loads, such as a large number of users making payments or filing claims simultaneously.

5. **Security Testing:**
   Security testing involves testing the system's security to ensure that it is protected against various security threats. For the insurance framework, this would involve testing the system's security against various threats, such as hacking, data breaches, and denial of service attacks.

6. **In conclusion**, testing is an essential part of the development of a secured insurance framework using blockchain and smart contract technology. By testing each module individually and then testing their interactions together, the system can be ensured to be efficient, secure, and transparent. Testing the system's performance and security is also crucial to ensure that it can handle a large number of transactions and is protected against various security threats.

5.3.2: TEST RESULTS OF VARIOUS STAGES

1. **UNIT TESTING:**

   In the unit testing stage, each module of the system would be tested individually to ensure that it meets its specified requirements. Some expected results of this stage include:

   - The smart contract module is able to initialize, issue, and process claims and refunds efficiently.
   - The payment gateway integration module is able to process payments securely and efficiently.
   - The identity verification module is able to verify the identity of various users using different verification methods accurately and efficiently.
   - The insurance pool module is able to manage funds efficiently and handle a large number of claims.

2. **INTEGRATION TESTING:**

   In the integration testing stage, the interactions between different modules of the system would be tested to ensure that they work together seamlessly. Some expected results of this stage include:

   - The smart contract module, payment gateway integration module, identity verification module, insurance pool module, user interface module, and blockchain network module work together efficiently and without any errors.
   - The system is able to process user requests accurately and efficiently.
   - Transactions and data are stored securely and transparently on the blockchain network.

3. **SYSTEM TESTING:**

   In the system testing stage, the entire system would be tested to ensure that it meets the specified requirements. Some expected results of this stage include:

   - The entire process of registering for a policy, making payments, filing claims, and receiving payouts is efficient, secure, and transparent.
   - User data is stored securely and transparently on the blockchain network.
   - The system is able to handle a large number of transactions and users simultaneously without any performance issues.

4. **PERFORMANCE TESTING:**

In the performance testing stage, the system's performance would be tested under various loads to ensure that it can handle a large number of transactions without any performance issues. Some expected results of this stage include:

- The system is able to handle a large number of transactions and users simultaneously without any performance issues.
- Transactions are processed efficiently and without any delays.
- The system is able to handle peak loads during busy periods, such as during natural disasters or other emergencies.

5. **SECURITY TESTING:**

In the security testing stage, the system's security would be tested to ensure that it is protected against various security threats. Some expected results of this stage include:

- The system is protected against hacking, data breaches, and other security threats.
- User data and transactions are stored securely and transparently on the blockchain network.
- The system is able to detect and prevent fraudulent activities, such as false claims or identity theft.

Overall, the expected results of testing the secured insurance framework using blockchain and smart contract technology are a more efficient, secure, and transparent insurance system that is able to handle a large number of transactions and users simultaneously, protect against various security threats, and provide accurate and timely payouts to clients.

5.3.3: CONCLUSION OF TESTING:

To summarize, it is essential to test the secure insurance framework using blockchain and smart contract technology to ensure that the system is efficient, secure, and transparent. The testing process comprises several stages, such as unit testing, integration testing, system testing, performance testing, and security testing, which are instrumental in identifying potential issues or weaknesses in the system and ensuring that it meets all specified requirements.

Through testing, we can expect the system to be able to handle a large number of transactions and users simultaneously without any performance issues, store user data and transactions securely and transparently on the blockchain network, and protect against various security threats. The system is also expected to provide accurate and timely payouts to clients while minimizing fraudulent activities, such as false claims or identity theft.

Overall, the testing of the secured insurance framework using blockchain and smart contract technology is essential to ensure that the system meets the needs and expectations of its clients and provides a more efficient, secure, and transparent insurance experience.

5.4: SUCCESS OF SYSTEM

The success of the secured insurance framework using blockchain and smart contract technology can be measured by several factors, including its efficiency, security, and transparency.

- **EFFICIENCY:**
  The system should be able to process a large number of transactions and users simultaneously without any performance issues. It should also automate various insurance processes, such as policy initialization, issuing, claiming, and refunds, to minimize human error and speed up the process.

- **SECURITY**
  The system should be designed to protect user data and transactions from unauthorized access, manipulation, or deletion. It should also be resistant to various security threats, such as hacking, DDoS attacks, and fraud. The use of blockchain technology can help ensure the system's security by decentralizing data storage and implementing a consensus mechanism to verify transactions.

- **TRANSPARENCY:**
  The system should provide transparent access to user data and transactions, allowing clients to verify their policy details, claims, and refunds. The use of smart contracts can help automate insurance processes and enforce policy rules transparently, ensuring that clients receive accurate and timely payouts.

If the system meets these criteria and provides a more efficient, secure, and transparent insurance experience for its clients, it can be considered successful. Additionally, if the system is widely adopted by the insurance industry and positively impacts the insurance market by reducing costs and improving customer satisfaction, it can be considered a significant success.

CHAPTER 6: CONCLUSION & FUTURE IMPROVEMENTS

6.1 CONCLUSION:

This study aims to present an insurance smart contract architecture built on the blockchain. An extremely secure private, decentralized system based on Ethereum is used to conduct insurance transaction processes. The conventional insurance contracts are created in this architecture using smart contracts. The decentralized Solidity smart contracts employed in this system streamline the insurance and claim settlement procedures due to their immutability. By utilizing the PoA algorithm in this design, money and storage are saved. As a result, the framework offers an effective and secure means of conducting business in the insurance sector.

6.2 PERFORMANCE ESTIMATION

The performance estimation of the secured insurance framework using blockchain and smart contract technology can be done by considering several factors, including transaction throughput, response time, scalability, and resource utilization.

6.2.1 TRANSACTION THROUGHPUT:

The transaction throughput refers to the number of transactions the system can handle per second. In the case of the secured insurance framework, it is essential to ensure that the system can handle a large number of policy initialization, issuing, claiming, and refund transactions simultaneously. The transaction throughput can be improved by optimizing the blockchain network's consensus algorithm, reducing the block size, and optimizing smart contract code.

6.2.2 RESPONSE TIME:

The response time refers to the time it takes for the system to respond to a user request. In the case of the secured insurance framework, it is crucial to ensure that the system can respond to user requests in a timely manner, such as policy initialization, issuing, claiming, and refunds. The response time can be improved by optimizing the smart contract code and ensuring that the blockchain network's consensus algorithm is efficient.

6.2.3 SCALABILITY:

The scalability of the system refers to its ability to handle a growing number of users and transactions. In the case of the secured insurance framework, it is essential to ensure that the system can handle a growing number of clients and insurance policies.

The scalability can be improved by optimizing the smart contract code, increasing the number of nodes in the blockchain network, and implementing sharding.

6.2.4 RESOURCE UTILIZATION:

The resource utilization refers to the amount of computing power, memory, and storage space the system consumes. In the case of the secured insurance framework, it is essential to ensure that the system can operate within the available resources, such as server hardware or cloud infrastructure. The resource utilization can be improved by optimizing the smart contract code, reducing the blockchain network's storage requirements, and implementing off-chain solutions for non-critical operations.

Overall, the performance estimation of this technology should ensure that the system can handle a large number of transactions, respond to user requests in a timely manner, scale to handle a growing number of users, and operate within available resources.

6.3: USABILITY OF PRODUCT / SYSTEM

The usability of this technology is an essential aspect to consider to ensure its successful adoption by the insurance industry and its clients. Usability refers to the ease with which users can interact with the system, access its features and functionality, and perform various tasks.

Some of the key usability factors that should be considered for the secured insurance framework include:

6.3.1 USER-FRIENDLY INTERFACE:

The system needs to feature an intuitive and user-friendly interface that enables users to easily navigate and perform various tasks, such as registering, initiating, issuing, claiming, and refunding policies. The interface must be designed with the users' needs and preferences in mind, and it must be easily accessible from a range of devices and platforms.

6.3.2 CLEAR AND CONCISE INFORMATION:

The system should provide clear and concise information about policies, claims, and refunds, helping users understand the insurance processes and policies. The information should be presented in a structured and organized manner, making it easy for users to access and comprehend.

6.3.3 EFFICIENT AND AUTOMATED PROCESSES:

The system should automate various insurance processes, such as policy initialization, issuing, claiming, and refunds, to minimize human error and speed up the process. The system should also provide instant policy quotes and payouts, helping users save time and effort.

6.3.4 INTEGRATION WITH THIRD-PARTY SERVICES:

The system ought to connect with external services, like payment gateways, identity verification providers, and analytics software, in order to improve its capabilities and deliver users a smooth experience.

6.3.5 SECURITY AND PRIVACY:

The system should protect the security and privacy of user data and transactions, applying various security measures, e.g. encryption, multi-factor authentication, and access control.

Overall, the usability of the secured insurance framework is crucial to ensure its successful adoption by the insurance industry and its clients. The system should provide a user-friendly interface, clear and concise information, efficient and automated processes, integration with third-party services, and robust security and privacy features.

6.4: LIMITATIONS

While this technology offers several benefits to the insurance industry, there are also some limitations that should be considered. These limitations include:

6.4.1 TECHNICAL COMPLEXITY:

The implementation of the secured insurance framework requires advanced technical expertise in blockchain and smart contract technology, which can be a barrier for smaller insurance companies and those with limited technical resources.

6.4.2 COST:

The development and maintenance of the secured insurance framework can be costly, especially for smaller insurance companies. The cost of implementing blockchain technology and smart contracts can also be higher than traditional insurance processes.

6.4.3 REGULATORY UNCERTAINTY:

The regulatory landscape for blockchain and smart contract technology is still evolving, which can create uncertainty for insurance companies in terms of compliance and legal requirements.

6.4.4 SCALABILITY:

The current blockchain technology infrastructure may not be able to support the scalability requirements of large insurance companies, which can limit the adoption of the secured insurance framework.

6.4.5 INTEROPERABILITY:

The integration of the secured insurance framework with existing insurance processes and systems may require significant effort, which can limit its interoperability and adoption.

Overall, while technology offers several benefits, such as enhanced security, transparency, and efficiency, there are also limitations that should be considered. These limitations include technical complexity, cost, regulatory uncertainty, scalability, and interoperability.

6.5 SCOPE OF IMPROVEMENT

As the world moves to web3 which compresses blockchain technology , that is decentralized and more secure than traditional technology and in industries such as insurance and claim this innovation helps in transparent process and establish the trust between the parties involved. As it is based on a decentralized block it is very hard to do fraud or vulnerable to any kind of malicious attack.

The secured insurance framework using blockchain and smart contract technology is an innovative solution that offers several benefits to the insurance industry. However, there is always scope for improvement, and some areas where the framework can be enhanced include:

6.5.1 SCALABILITY:

The current blockchain technology infrastructure may not be able to support the scalability requirements of large insurance companies. Therefore, there is a need to develop more scalable blockchain solutions that can support the increasing demands of the insurance industry.

6.5.2 INTEGRATION:

The integration of the secured insurance framework with existing insurance processes and systems may require significant effort, which can limit its interoperability and adoption. Therefore, efforts should be made to develop more seamless integration solutions that can facilitate the adoption of the framework.

6.5.3 COST:

The development and maintenance of the secured insurance framework can be costly, especially for smaller insurance companies. Therefore, there is a need to develop more cost-effective solutions that can make the framework more accessible to smaller players in the insurance industry.

6.5.4 REGULATORY COMPLIANCE:

The regulatory landscape for blockchain and smart contract technology is still evolving, which can create uncertainty for insurance companies in terms of compliance and legal requirements. Therefore, efforts should be made to develop more regulatory-compliant solutions that can facilitate the adoption of the framework.

6.5.5 USER INTERFACE:

The usability of the secured insurance framework is crucial to ensure its successful adoption by the insurance industry and its clients. Therefore, efforts should be made to develop more user-friendly interfaces that can enhance the user experience and improve the adoption rate of the framework.

Overall, while the technology offers several benefits, there is always scope for improvement. Some areas where the framework can be enhanced include scalability, integration, cost, regulatory compliance, and user interface. By addressing these areas, the framework can be made more accessible, cost-effective, and user-friendly, thereby enhancing its adoption by the insurance industry.

REFERENCES

[1] "Estimated Size of the Global Insurance Market 2020," https://www.statista.com/statistics/1192960/forecast-global-ins urance-market/

[2] E. M. Immergut, "Health policy," in *International Encyclopedia Of the Social & Behavioral Sciences*, pp. 6586–6591, Elseiver, Amsterdam, Netherlands, 2001.

[3] A. Narayanan, J. Bonneau, E. W. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press, Princeton, NJ, 2016.

[4] "Bitcoin.org," https://bitcoin.org/bitcoin.pdf.

[5] M. Lischke and B. Fabian, "Analyzing the bitcoin network: the first four years," *Future Internet*, vol. 8, no. 4, p. 7, 2016.

[6] Government Office for Science, "Distributed ledger technology: beyond block chain," in Government of United Kingdom, 2

[7] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[8] W. Tsai, R. Blower, Y. Zhu, and L. Yu, "A system view of financial blockchains," in *Proceedings of the 2016 IEEE Symposium On Service-Oriented System Engineering (SOSE)*, pp. 450–457, Oxford, UK, March 2016.

[9] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," *in Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics* (SMC), pp. 2567–2572, Banff, Canada, October 2017.

[10] J. Ellul and G. Pace, "Blockchain and the common good reimagined," 2019, https://arxiv.org/abs/1910.14415.

[11] O. Alfandi, S. Otoum, and Y. Jararweh, "Blockchain solution for iot-based critical infrastructures: byzantine fault tolerance," in Proceedings of the *NOMS 2020 - 2020 IEEE/IFIP* Network Operations and Management Symposium, Budapest, Hungary, April 2020.

[12] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "Blockchain and smart contracts for insurance: is the technology mature enough?" *Future Internet*, vol. 10, no. 2, 2018.

[13] H. Luo, M. Das, J. Wang, and J. C. P. Cheng, "Construction payment automation through smart contract-based blockchain framework," in *Proceedings of the 36th International Symposium on Automation and Robotics in Construction (ISARC*

2019), pp. 1254–1260, Banff Alberta, Canada, May 2019.

[14] S. N. Khan, F. Loukil, C. G. Ghedira, E. Benkhelifa, and A. H. Bani, “Blockchain smart contracts: applications, challenges, and future trends,” *Peer-to-PeerNetworking and Application*, vol. 14, pp. 1–25, 2021.

[15] M. Raikwar, S. Mazumdar, S. Ruj, S. G. Sen, A. Chattopadhyay, and K. Y. Lam, “A blockchain framework for insurance processes,” in *Proceedings of the 2018 9th IFIP International Conference On New Technologies, Mobility And Security (NTMS)*, pp. 1–4, Paris- France, February 2018.

[16] P. K. Singh, R. Singh, G. Muchahary, M. Lahon, and S. Nandi, “A blockchain-based approach for usage-based insurance and incentive in its,” in *Proceedings of the TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON)*, pp. 1202–1207, Kochi, India, October 2019.

[17] K. Sayegh, *Blockchain Application in Insurance and Reinsurance*, SKEMA Business School, Lille, France, 2018.

[18] N. Atzei, M. Bartoletti, and T. Cimoli, “A survey of attacks on ethereum smart contracts (SoK),” in *Proceedings of the International Conference on Principles of Security and Trust*, pp. 164–186, Uppsala, Sweden, April 2017.

[19] F. Holotiuk, F. Pisani, and J. Moormann, “Radicalness of blockchain: an assessment based on its impact on the payments industry,” *Technology Analysis & Strategic Management*, vol. 31, no. 8, pp. 915–928, 2019.

[20] P. Tasca, “Insurance under the blockchain paradigm,” in *Business Transformation Through Blockchain*, pp. 273–285, Springer International Publishing, Cham, Switzerland, 2019.

[21] Nath, “Data exchange platform to fight insurance fraud on blockchain,” in *Proceedings of the 2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)*, pp. 821–825, Barcelona, Spain, December 2016.

[22] W. Chen, Z. Xu, S. Shi, Y. Zhao, and J. Zhao, “A survey of blockchain applications in different domains,” in *Proceedings of the 2018 International Conference On Blockchain Technology And Application - ICBTA 2018*, Xi’an, China, December 2018.

ANNEXURE 1

Research Paper for the said project has been **accepted** in *"International Conference on Demystifying Emerging Trends in Green Technology" ICDETGT-2023.*

Paper Title:

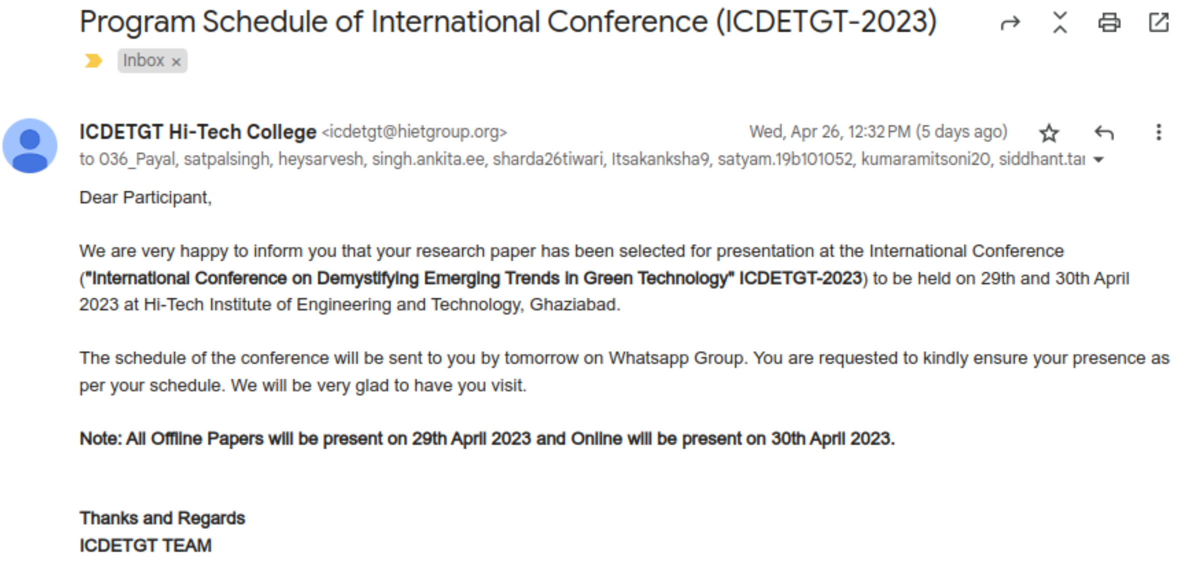
Insurance Framework Based on Blockchain and Smart Contract

Abstract:

Processing insurance claims requires a variety of human-agent interactions, multi-domain entities, and data from several sources. As a result, this procedure is typically time-consuming and labor-intensive. Platforms for intelligent automation built on blockchain technology can greatly increase the speed and scope of claims processing. Insurance policy claiming and settling is a complex process. This settlement process is challenging because of a variety of issues, such as hidden requirements from accusations of fraud by the client or the insurance body. The insurance sector could be completely transformed by the use of blockchain technology and smart contracts. The entire insurance processes, from verification to claim settlement, can be carried out with improved security and increased transparency with the adoption of blockchain technology. This paper gives a framework based on blockchain smart contracts for insurance. If all the requirements are fulfilled at the event of a claim, the transaction takes place; if not, it is rejected. To develop smart contracts, a programming language called Solidity is employed. The system makes use of the consensus algorithm known as Proof of Authority (PoA) for the validation of each transaction.

Authors:

Abhishek kumar Singh, Sahil Shivhare, Dr. Nishant Gupta.



Program Schedule of International Conference (ICDETGT-2023)

ICDETGT Hi-Tech College <icdetgt@hietgroup.org> Wed, Apr 26, 12:32 PM (5 days ago)

to 036_Payal, satpalsingh, heysarvesh, singh.ankita.ee, sharda26tiwari, ltsakanksha9, satyam.19b101052, kumaramitsoni20, siddhant.tai

Dear Participant,

We are very happy to inform you that your research paper has been selected for presentation at the International Conference (**"International Conference on Demystifying Emerging Trends in Green Technology" ICDETGT-2023**) to be held on 29th and 30th April 2023 at Hi-Tech Institute of Engineering and Technology, Ghaziabad.

The schedule of the conference will be sent to you by tomorrow on Whatsapp Group. You are requested to kindly ensure your presence as per your schedule. We will be very glad to have you visit.

Note: All Offline Papers will be present on 29th April 2023 and Online will be present on 30th April 2023.

Thanks and Regards
ICDETGT TEAM