IJITCE

ISSN 2347- 3657

# International Journal of Information Technology & Computer Engineering

www.ijitce.com

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 1, 2025

# Immutability of Block chain for the Development of Secure Robust Digital Communication Network

Dr. Puspita Dash1, Brindha Selvam2, Hari Sowmiyaa Arulmozhi Thamilarasan3, Ranetha Velavan4

1,2,3,4 Information Technology, Sri Manakula Vinayagar Engineering College, Madagadipet, Puducherry 605107, India

**Abstract - The paper, "CryptoStone: A Blockchain-Powered Communication Paradigm for Unparalleled Immutability", seeks to revolutionize secure and reliable communication protocols. At its essence, the system leverages blockchain to establish unparalleled levels of immutability and transparency in digital interactions. Operating within a decentralized architecture, communication events are encapsulated into blocks, each one is cryptographically linked to its predecessor. The distributed nature of the network helps to make sure there is no single point of failure or vulnerability, markedly enhancing security. Employing advanced cryptographic techniques and consensus algorithms, the proposed system not only safeguards the integrity of messages, files, and multimedia but also creates an auditable trail of communication events. This innovative approach proves particularly advantageous in sectors where the accuracy of communication records is critical, such as legal proceedings, financial transactions, or healthcare documentation. By introducing a novel paradigm for communication integrity, the project envisions a future where the immutable nature of blockchain becomes foundational for constructing resilient, secure, and trustworthy digital communication ecosystems. The paper mentions the use of merkle tree for ensuring integrity of the data and how it helps to deflect attacks made towards it. In essence, this endeavor represents a pioneering stride towards a future where the immutability of blockchain is central to the development of robust and secure digital communication frameworks.**

**Keywords:-Immutability, data integrity, cryptographic hashes, PatriciaMerkle tree, web 3.0, decentralization.**

## I. INTRODUCTION

In the dynamic realm of digital communication, the introduction of blockchain technology and decentralized systems signifies a pivotal shift towards enhanced security, transparency, and a user-centric approach. Traditional communication applications, rooted in centralization, have long grappled with vulnerabilities, spanning from potential data breaches to privacy issues. Despite existing applications like Cryptouch and Crypviser leveraging blockchain for communication, they are not without drawbacks. This paper delves into the potential of a decentralized communication system founded on Web 3.0 principles, utilizing blockchain to revolutionize the benchmarks of secure and unalterable digital communication. Moreover, it addresses the challenges prevalent in current systems, offering innovative solutions for a more robust and effective communication paradigm.

### A. Block chain :

Block chain is a type of distributed technology which allows for decentralization of our data, it also allows multiple parties to record and store their data without any need for centralized database. It revolutionizes the way transactions are recorded and verified without the need for a central authority. Its roots can be traced back to 1991 when Stuart Haber and W. Scott Stornetta conceptualized a cryptographically secure chain of blocks. However, the term "block chain" gained prominence with Satoshi Nakamoto's introduction in the context of Bitcoin, detailed in the 2008 whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System.". The Figure 1 shows the architecture of the block chain technology.

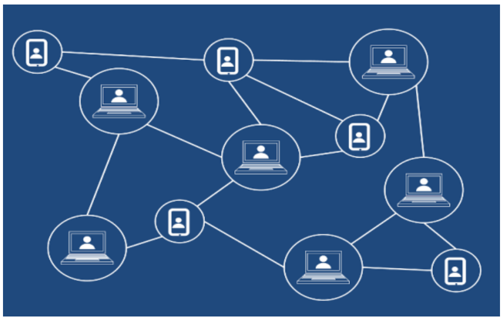


**Fig. 1. BLOCKCHAIN TECHNOLOGY**

The blockchain mechanism operates as a decentralized and distributed ledger system that ensures secure and transparent record-keeping across a network of computers. Key concepts include:

### B. Block chain key concepts and mechanism :

The block chain mechanism is a type of ledger system which is both distributed and decentralized in nature. It helps us to keep track of data and various transactions with the help multiple nodes available across various networks of computers. It's core concepts involve blocks, cryptographic hashes, concensus mechanisms, and decentralization.

1. Blocks:

Transactions are organized into blocks, each containing a list of transactions. These blocks reference the previous one, forming an unbroken chain. This chaining maintains the integrity of the entire transaction history.

2. Decentralization:

In contrast to centralized systems, blockchain operates on a decentralized network where multiple nodes maintain a copy of the entire blockchain. This enhances security, resilience, and eliminates a single point of failure.

3. Cryptographic Hashes:

Blocks are linked through cryptographic hashes—unique identifiers generated by hash functions. These hashes depend on block content, including the hash of the previous block. Any attempt to tamper with a block alters the hash, revealing the tampering.

4. Consensus Mechanisms:

Block chain networks employ consensus mechanisms to validate transactions and determine their order in the block chain. Proof of Work (used by Bitcoin) involves solving complex puzzles, while alternatives like Proof of Stake and Delegated Proof of Stake offer different consensus approaches.

5. Smart Contracts:

Ethereum introduced smart contracts, self-executing agreements with terms encoded into code. They automatically execute and enforce agreed-upon terms when specific conditions are met, reducing the need for intermediaries.

6. Immutability:

Once a block is added, its content is resistant to alteration due to cryptographic hashes and the decentralized network. This immutability ensures the security and tamper-proof nature of historical records.

7. Transparent and Public Ledger:

Block chain ledgers are often public and transparent, enabling anyone to view the entire transaction history. However, transparency levels may vary based on the block chain type (public, private, or consortium). Block chain's impact extends across industries, with enterprises recognizing its potential to enhance processes, security, and reduce fraud. Consortium and private block chains have emerged, and different consensus mechanisms address energy consumption concerns. Interoperability solutions and scalability enhancements aim to facilitate communication and overcome transaction throughput limitations in diverse block chain networks. In the realm of block chain technology, decentralization stands as a fundamental principle, seeking to disperse control and decision-making among a network of participants instead of depending on a central authority. The process of achieving decentralization involves multiple stages, and the utilization of a Patricia Merkle tree emerges as a pivotal element in preserving data integrity and optimizing efficiency within this framework.

### C. Steps in Decentralization Mechanism:

1. Network Nodes:

The system has multiple node systems (computers) which are the ones participating in our network. Each one of these nodes maintains a copy of the whole block chain ledger.

2. Transaction Propagation:

Upon the initiation of a transaction by a participant, it is disseminated across the network. Nodes within the network then undertake the validation of the transaction, ensuring its precision and compliance with consensus rules.

3. Block Formation:

Each of these valid transactions are grouped together into a single block.Nodes compete to solve a cryptographic puzzle (Proof of Work, Proof of Stake, etc.) in order to add these blocks to a block chain network.

4. Consensus Mechanism:

Nodes reach consensus on the validity of transactions and agree on the next block. This agreement is crucial for maintaining a consistent and accurate ledger across all nodes.

5. Block Addition:

The victorious node transmits the newly formed block to the network. Subsequent to this, other nodes authenticate the block's validity before incorporating it into their respective copies of the blockchain.

6. Blockchain Update:

Each node updates its local copy to the blockchain network. It ensures that all of the nodes in the block consists of the same transaction history.

**D. Patricia Merkle Tree in Decentralization:**

A Patricia Merkle tree, a variation of the Merkle tree, is a modified data structure designed to effectively confirm the integrity and coherence of extensive datasets. Within the framework of decentralization, Patricia Merkle trees find frequent application in structuring and presenting data within individual blocks of the blockchain. The operational process is as follows:

1. Data Organization:

Transactions within a block are structured in the form of a Merkle tree. Each leaf node corresponds to a single transaction, while non-leaf nodes consist of hashes derived from their respective child nodes..

2. Hashing Layers:

The Merkle root, situated at the pinnacle of the Merkle tree, is included in the block header and serves as a cryptographic hash uniquely representing all the transactions within the block.

3. Efficient Verification:

Confirming the integrity of a specific transaction or a set of transactions is streamlined through Merkle trees. Participants can validate a transaction's inclusion by examining a series of hashes from the transaction to the Merkle root.

4. Compact Representation:

Patricia Merkle trees optimize storage by condensing shared prefixes in the tree. This compression reduces the volume of data to be transmitted and stored, thereby enhancing the efficiency of the blockchain.

By integrating Patricia Merkle trees, blockchain networks bolster the security, efficiency, and integrity of data storage. This structural implementation ensures that even a minor alteration in a transaction necessitates changes to the corresponding Merkle path and the Merkle root, making any tampering detectable by the network.

## II. LITERATURE SURVEY

### A. A Block chain Ontology for DApps Development

In this paper the authors introduce a comprehensive framework for developing Decentralized Applications (DApps) through the utilization of block chain ontology. [1] The primary goal of this research is to provide a structured and standardized approach to DApps development by leveraging block chain ontology. The paper meticulously details the methodology of the proposed framework, emphasizing its innovative use of ontology to enhance the development, interoperability, and understanding of DApps within the block chain ecosystem. One notable advantage of this approach is its potential to establish a common language and framework for DApps development, fostering collaboration and consistency in the decentralized application landscape. However, challenges may include addressing the complexity of integrating ontology into block chain development workflows and ensuring widespread adoption within the block chain community. This research significantly contributes to the field by providing a foundational framework for DApps development, aligning with the need for structured and interoperable solutions in the block chain domain.

### B. Block chain-Based Decentralized Application: A Survey

In this paper the authors conduct an extensive examination of the landscape of decentralized applications (DApps) built on blockchain technology.[2] The primary objective of this research is to provide a comprehensive overview and analysis of the current state of blockchain-based DApps. The paper meticulously details the survey methodology, emphasizing its systematic exploration of various aspects, including development trends, use cases,challenges, and future directions in the realm of decentralized applications. One notable advantage of this approach is its potential to offer a holistic understanding of the diverse applications and challenges associated with blockchain based DApps.

| S.NO. | PAPER TITLE | TECHNIQUES USED | DRAWBACKS |
|---|---|---|---|
| 1 | A Blockchain Ontology for DApps Development, 2022 | The paper's method involves developing Decentralized Applications (DApps) through a comprehensive framework that utilizes blockchain ontology | The text does not specify any explicitly mentioned disadvantages or challenges associated with the proposed framework in the paper. |
| 2 | A study on the challenges and solutions of blockchain interoperablity ,2023 | The paper thoroughly examines challenges and proposes solutions for blockchain interoperability. It systematically analyzes technical, architectural, and consensus-related issues. | While not explicitly mentioned, there's a challenge in keeping up with the dynamic nature of blockchain technology, requiring ongoing efforts to stay updated with emerging developments. |
| 3 | A Block Chain and Cryptography based Secure Communication System, 2023 | The paper suggests a secure communication system based on the collaboration of cryptography techniques and blockchain for heightened security. | The incomplete implementation of the system implies that practical testing and real-world application are necessary to evaluate the effectiveness and feasibility of this secure communication system based on blockchain and cryptography. |
| 4 | Promoting the Sustainability of Blockchain in Web 3.0 and the Metaverse Through Diversified Incentive Mechanism Design, 2023 | The paper suggests ways to make blockchain sustainable in advanced Web environments. It recommends a diverse incentive system to encourage sustainable practices. | The challenge is finding the right balance between motivating users and keeping the blockchain network secure for long-term success. |
| 5 | Blockchain Based Secure Communication for IoT Devices in Smart Cities, 2019 | The system employed three-node blockchains created with the JSON library. Communication across the network was facilitated using the Socket library and the UDP protocol. To secure the communication in the UDP-based system, the Vigenere cipher encryption method was utilized for message encryption. | The project encountered communication challenges attributed to the UDP protocol. Notably, upon the closure and subsequent reopening of any node within the project, it was noted that the blocks added to the blockchain of other nodes were appended to their respective blockchains during the reopening process |
| 6 | Graph Coded Merkle Tree: Mitigating Data Availability Attacks in Blockchain Systems Using Informed Design of Polar Factor Graphs, 2023 | The paper deals with attacks on data availability in blockchains using a new idea called Graph Coded Merkle Tree. It aims to make blockchain systems more secure against attempts to compromise data availability. | The tricky part is that it might be hard to add this new idea to existing blockchains. Making it work in different setups could be complex. |

### C. A study on the challenges and solutions of blockchain interoperability

In this paper the authors undertake a thorough examination of the obstacles and potential remedies associated with achieving interoperability in the realm of blockchain technology. [3] This research paper extensively explores challenges and solutions in achieving blockchain interoperability. It systematically analyzes technical, architectural, and consensus-related issues, presenting innovative solutions. By demanding continuous efforts to stay updated on emerging developments, the discoveries in this research provide practical guidance for developers and stakeholders, making a significant contribution to navigating the ever-evolving landscape of blockchain technology. This research significantly contributes to the field by offering a valuable resource for addressing the complexities of blockchain interoperability, aligning with the growing need for seamless collaboration among diverse blockchain networks.

### D. A Block Chain and Cryptography based Secure Communication System

Kokkonda Shiva Kumar et al [4] proposed a secure communication system based on the collaboration of cryptography techniques and blockchain for heightened security. Despite the potential advantages of combining these technologies, it's important to note that the system has not been fully implemented as of the provided information. The lack of full implementation suggests that practical testing and real-world application may be required to assess the effectiveness and viability of this blockchain and cryptography-based secure communication system.

### E. Promoting the Sustainability of Blockchain in Web 3.0 and the Metaverse Through Diversified Incentive Mechanism Design

In this paper the authors delve into strategies aimed at enhancing the sustainability of blockchain technology within the evolving landscapes of Web 3.0 and the Metaverse.[5] The primary goal of this research is to propose a diversified incentive mechanism design that fosters sustainable practices in blockchain ecosystems. The paper meticulously details the methodology of incentive mechanism design, emphasizing its innovative approach to address the unique challenges posed by the integration of blockchain in advanced web environments. One notable advantage of this approach is its potential to encourage diverse and sustainable participation within blockchain networks, aligning with the principles of decentralization and longevity. However, challenges may include striking a balance between incentivizing users and maintaining the integrity of the blockchain network. This research significantly contributes to the field by offering a conceptual framework for sustainable blockchain practices in the context of Web 3.0 and the Metaverse.

### F. Blockchain Based Secure Communication for IoT Devices in Smart Cities

In this paper the authors Ramazan Yetis et al [6] proposed enhacing communication of IOT devices using blockchain technology. This addresses the challenge of secure communication for Internet of Things (IoT) devices in smart cities by proposing a blockchain-based solution. The current approach involves the utilization of the User Datagram Protocol (UDP) instead of traditional Internet Protocol (IP) protocols. However, the reliance on UDP introduces security concerns, particularly in the form of unsafe communication. The content of UDP packets is transmitted without encryption, posing a potential risk to the confidentiality and integrity of the communicated data.

### G. Graph Coded Merkle Tree: Mitigating Data Availability Attacks in Blockchain Systems Using Informed Design of Polar Factor Graphs

In this paper the authors tackle the issue of data availability attacks in blockchain systems through the introduction of a novel concept called Graph Coded Merkle Tree. [7] The primary objective of this research is to propose a robust solution to enhance the security and resilience of blockchain systems against malicious attempts to compromise data availability. The paper meticulously details the informed design of polar factor graphs as a key component of the Graph Coded Merkle Tree, emphasizing its potential to mitigate data availability attacks effectively. One notable advantage of this approach is its ability to provide a structured and resilient data structure that enhances the fault tolerance of blockchain networks. However, challenges may include the complexity of implementing graph coding within existing blockchain infrastructures. This research significantly contributes to the field by presenting a novel technique for safeguarding data availability in blockchain systems.

### H. Multi-State Merkle Patricia Trie (MSMPT): High-Performance Data Structures for Multi-Query Processing Based on Lightweight Blockchain

In the paper titled "Multi-State Merkle Patricia Trie (MSMPT) the authors delve into the development of a novel data structure, the Multi-State Merkle Patricia Trie (MSMPT), designed to enhance the efficiency of multi-query processing in lightweight blockchain systems.[8] The primary objective solution statement of this research is to introduce a high-performance data structure that addresses the challenges associated with processing multiple queries within a lightweight blockchain environment. The paper meticulously details the design principles and features of the MSMPT, highlighting its potential to improve the speed and resource utilization for handling multiple queries concurrently. One notable advantage of this approach is its ability to provide a streamlined and efficient solution for data storage and retrieval in lightweight blockchains, potentially leading to improved overall system performance. However, challenges may include the need for compatibility with existing systems.

## III. EXISTING SYSTEM

The existing solutions for communication systems, largely rooted in Web 2.0 technologies, are predominantly centralized. Popular chat applications operate on centralized servers, where user data, messages, and communication logs are stored in a singular, controlled location. While these platforms offer convenience and widespread accessibility, they inherently carry vulnerabilities. Centralized systems are susceptible to data breaches, as a single point of failure could compromise the entire network. Moreover, the reliance on a central authority for data management raises concerns about user privacy, as these entities have access to sensitive information. The immutability of communication records is challenging to guarantee in such environments, as data can be altered or manipulated with administrative access. The proposed project seeks to address these shortcomings by embracing the decentralized and tamper-resistant nature of blockchain, providing a robust alternative to the current centralized paradigm and redefining the standards for secure, trustworthy, and immutable digital communication.

In response to the inherent challenges associated with smart contracts in decentralized chat applications, we are proposing a transformative solution that aims to mitigate these drawbacks by leveraging the Patricia Merkle Tree concept. Unlike the conventional reliance on smart contracts for handling transactions and logic execution, our approach introduces a decentralized data structure in the form of a Patricia Merkle Tree. This tree structure enhances efficiency in verifying the integrity of chat data, ensuring secure and tamper-resistant communication within the decentralized application (DApp). By transitioning away from the limitations of smart contracts, this innovative approach addresses concerns such as immutability, scalability challenges, and the complexity of execution, offering a more flexible and scalable foundation for decentralized chat applications. The Patricia Merkle Tree not only streamlines data verification but also facilitates a more modular and adaptable architecture, allowing for dynamic updates and improved privacy while maintaining the decentralized ethos of DApps. This paradigm shift represents a significant advancement in the development of secure and scalable decentralized chat applications.Below are some of the projects previously published.

A. Crypviser:

Crypviser stands out as a highly secure messaging app built on Blockchain technology. The decentralized Crypviser Messenger offers users the ability to engage in private video chats and voice calls with automatic blockchain encryption.

However, it is not without its drawbacks, including concerns about data security at the local database level, potential issues related to accessing data embedded in QR codes, decryption challenges, and the possibility of intercepting communications between users. Other mentioned vulnerabilities encompass Man-in-the-Middle (MiTM) attacks, which could involve intercepting and substituting public keys for deceptive messaging. Additionally, there are noted concerns about the decryption of messages exchanged between users and bots. Despite its appearance as a communication application, CrypViser seems to prioritize the sending of cryptocurrency coins as its primary function.

B. Cryptouch:

The primary objectives include the following:

- Delivering an intermediary, distributed, open-source, secure, transparent, and uninterrupted communication experience to users, aligned with its free software philosophy.
- Achieving a user-to-user messaging, file transfer, video meeting, and announcement system without mediation, leveraging innovative technologies like IPFS.

The primary drawback is the absence of group sharing messages, and as of now, the platform has not been released for public users. It appears that the project is still in its initial stages of development. C. Block Chain and Cryptography based Secure Communication System:

Block chain technology has emerged as a critical focus area for all multinational organizations' development in recent years, with a great number of startups emerging in this industry. This study covers current block chain challenges and presents cryptography's major uses. To begin, the block chain technology, starting with the block chain infrastructure, is simplified. Second, to better understand the block chain, Cryptography technology is offered. Finally, the Block chain's current security weaknesses are evaluated. It demonstrates that digital encryption is employed throughout the block chain system and is a necessary component. For maximum security, the communication system's message will be transmitted via encryption and the block chain protocol. Future plans include developing and deploying social media tools, particularly for communication. Encryption techniques are now used in every system. As a result, in the future, block chain and encryption will combine for more privacy.

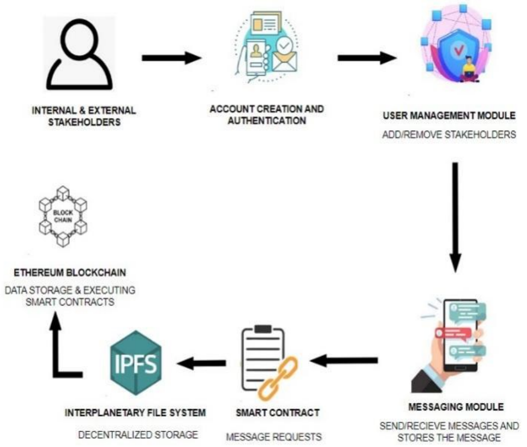

INTERNAL & EXTERNAL STAKEHOLDERS
ACCOUNT CREATION AND AUTHENTICATION
USER MANAGEMENT MODULE
ADD/REMOVE STAKEHOLDERS
BLOCK CHAIN
ETHEREUM BLOCKCHAIN
DATA STORAGE & EXECUTING SMART CONTRACTS
IPFS
INTERPLANETARY FILE SYSTEM
DECENTRALIZED STORAGE
SMART CONTRACT
MESSAGE REQUESTS
MESSAGING MODULE
SEND/RECIEVE MESSAGES AND STORES THE MESSAGE

**Fig. 2.**

## IV. PROPOSED SOLUTION

### A. PROBLEM SOLUTION

The proposed solution involves creating a decentralized communication system based on the principles of Web 3.0, aiming to overcome the limitations seen in current centralized applications. Through the utilization of blockchain technology and decentralization, our system fundamentally shifts the existing paradigm. Within this decentralized application (dApp), user communications are spread across a network of nodes, eliminating vulnerabilities associated with a single point of control. Smart contracts and cryptographic hashing are employed to ensure the integrity and immutability of communication records. Participants in the network maintain ownership and control over their data, thus enhancing privacy and security. The absence of a central authority minimizes the risk of data breaches, as no single entity possesses comprehensive access. This innovative approach not only addresses security concerns but also aligns with the principles of Web 3.0, fostering a user-centric and trustless environment. Our solution aims to lead a new era in digital communication by seamlessly integrating decentralized principles, thereby establishing a robust, transparent, and tamper-resistant framework for the exchange of information.

### B. PROPOSED SYSTEM ARCHITECTURE

In our "Immutable Communication System (DApp) Using Blockchain" architecture, we are first greeted with account creation and authentication, after which comes several other modules such as account management module, messaging module, storage module, etc. Here storage is done with the help of IPFS system. Afterwards the node is added to the Ethereum blockchain as another block. The Figure 2 shows the System architecture of the proposed work.

**Fig.2. SYSTEM ARCHITECTURE**

### C. MODULES

#### 1. Authentication Module:

In our "Immutable Communication System (DApp) Using Blockchain" project, User authentication serves as a trusted and user-friendly way for individuals to prove who they are and securely interact with our decentralized communication platform. Transaction Layer Security(TLS) PKI enables strong authentication by using asymmetric key pairs. Each user has a public key, which is shared openly, and a private key, which is kept secret. This ensures that the party at the other end of the communication is who they claim to be. It acts as a digital keychain. When the user wants to access our communication system, tis digital keychain asks them to unlock their digital key, proving they are who they say they are.

By this Authentication Module users have control over their information, and their interactions remain safe and protected on the blockchain.

#### 2. Account Management Module:

The account management module plays a pivotal role in ensuring the secure management of user registrations and account details. This module not only facilitates secure interactions but also empowers users to personalize their profiles. This includes the option to update profile pictures and display names, contributing to the creation of a tailored and secure communication experience for each user.

**Account Details Administration**: It is responsible for managing and safeguarding user account details, guaranteeing the confidentiality and integrity of sensitive information.

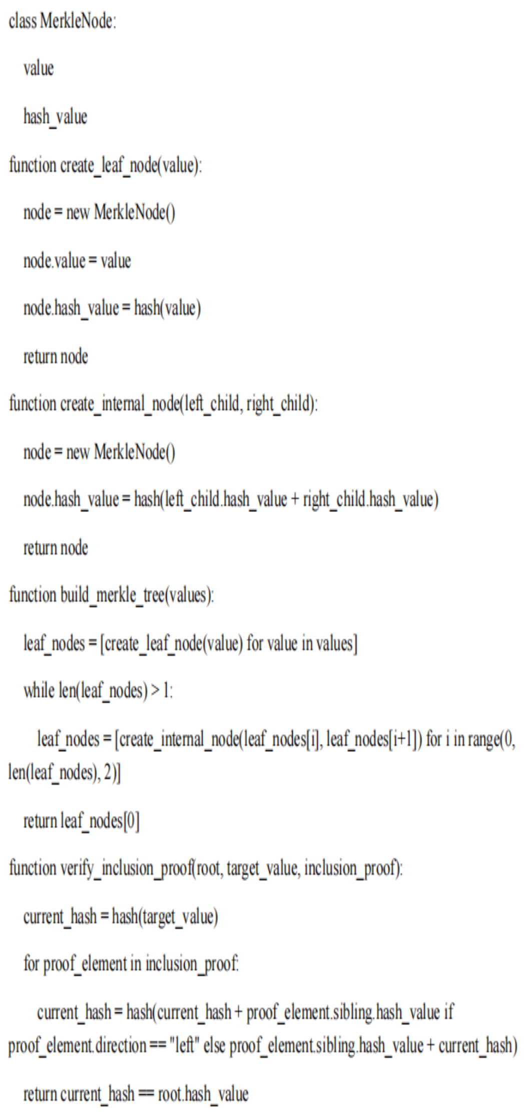
**Profile Personalization:** Users can customize their profiles through the module, allowing them to update profile pictures and display names, fostering a personalized user experience.

**Secure Interactions**:The module facilitates secure interactions between users, implementing measures to protect the confidentiality of communications and sensitive data.

### 3. Messaging Module:

This module allows you to communicate with friends and colleagues on the platform. When you send a message, it gets stored securely on the blockchain and can't be tampered with. IPFS adds an extra layer of protection, making sure your messages are stored in a really safe and hard-to-touch way, making our communication system extra reliable and secure. Additionally, this module explores decentralized storage solutions like IPFS, adding an extra layer of security to the way messages are stored and retrieved. We are using Transport Layer Security (TLS), which is a cryptographic protocol designed to secure communication over a computer network. It is widely used to secure data transmission on the internet, providing privacy and data integrity between communicating applications.

### 4. Storage Module:



```
class MerkleNode:
  value
  hash_value
function create_leaf_node(value):
  node = new MerkleNode()
  node.value = value
  node.hash_value = hash(value)
  return node
function create_internal_node(left_child, right_child):
  node = new MerkleNode()
  node.hash_value = hash(left_child.hash_value + right_child.hash_value)
  return node
function build_merkle_tree(values):
  leaf_nodes = [create_leaf_node(value) for value in values]
  while len(leaf_nodes) > 1:
    leaf_nodes = [create_internal_node(leaf_nodes[i], leaf_nodes[i+1]) for i in range(0,
len(leaf_nodes), 2)]
  return leaf_nodes[0]
function verify_inclusion_proof(root, target_value, inclusion_proof):
  current_hash = hash(target_value)
  for proof_element in inclusion_proof:
    current_hash = hash(current_hash + proof_element.sibling.hash_value if
proof_element.direction == "left" else proof_element.sibling.hash_value + current_hash)
  return current_hash == root.hash_value
```

The Storage Module in our project, coupled with IPFS (InterPlanetary File System), serves as a secure and decentralized repository for vital information, such as messages. IPFS, acting like a super-smart storage system, breaks down messages into tiny pieces and scatters them across multiple computers.

These IPFS uses cryptographic hashing which ensures data integrity, and the content-addressable approach allows for efficient retrieval based on the unique identifier of the content.This ensures that messages are not only securely stored but also highly resistant to tampering. The Storage Module works hand-in-hand with IPFS, creating an organized and reliable system where each piece of information has its secure spot in this decentralized vault.

### D. ALGORITHMS USED

We are using a patricia merkle tree based tree like datastructure  to efficiently store and retrieve key-value pairs within a distributed database. This structure combines aspects of both Merkle Trees and Patricia Tries.

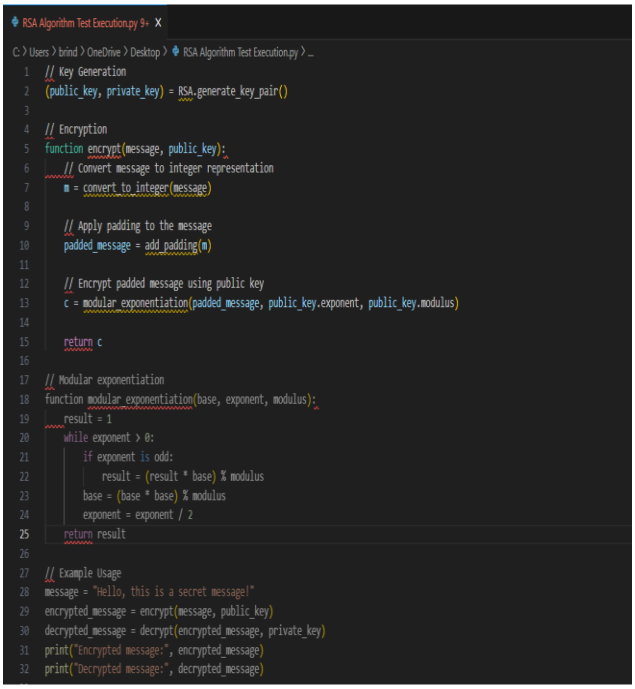
**ALGORITHM 1: PATRICIA MERKLE TREE FOR DATA**

## V. RESULT & DISCUSSION

### LOGIN AND AUTHENTICATION

In this application has been encrypted with the help of RSA algorithm. The RSA algorithm (Rivest-Shamir-Adleman) is the basis of a cryptosystem -- a suite of cryptographic algorithms that are used for specific security services or purposes -- which enables public key encryption and is widely used to secure sensitive data, particularly when it is being sent over an insecure network such as the internet.

Moreover, RSA is integral to the implementation of digital signatures, allowing participants to sign transactions with their private keys, validating the authenticity and integrity of data transmitted across the blockchain network. This digital signature mechanism not only verifies the identity of participants but also safeguards transactions from tampering or unauthorized alterations. Additionally, RSA facilitates secure key exchange protocols, bolstering the establishment of secure communication channels and enabling the exchange of session keys for symmetric encryption methods. Overall, RSA plays a pivotal role in fortifying the security framework of blockchain-based communication networks, fostering trust, integrity, and confidentiality among participants while mitigating the risks posed by malicious actors. The Figure 3 shows the execution of RSA encryption algorithm.


RSA Algorithm Test Execution.py 9+ X
C: › Users › brind › OneDrive › Desktop › RSA Algorithm Test Execution.py › ...

```
// Key Generation
(public_key, private_key) = RSA.generate_key_pair()

// Encryption
function encrypt(message, public_key):
    // Convert message to integer representation
    m = convert_to_integer(message)

    // Apply padding to the message
    padded_message = add_padding(m)

    // Encrypt padded message using public key
    c = modular_exponentiation(padded_message, public_key.exponent, public_key.modulus)

    return c

// Modular exponentiation
function modular_exponentiation(base, exponent, modulus):
    result = 1
    while exponent > 0:
        if exponent is odd:
            result = (result * base) % modulus
        base = (base * base) % modulus
        exponent = exponent / 2
    return result

// Example Usage
message = "Hello, this is a secret message!"
encrypted_message = encrypt(message, public_key)
decrypted_message = decrypt(encrypted_message, private_key)
print("Encrypted message:", encrypted_message)
print("Decrypted message:", decrypted_message)
```

**Fig.3. RSA ENCRYPTION ALGORITHM EXECUTION**

In this work, utilizing a combination of RSA and patricia merkle tree algorithm in order to make our transaction secure and robust. We are integrating Merkle Trees into our blockchain based communication system for data integrity, efficient storage enhancing the security and consistency of a blockchain-based communication system by enabling quick verification of data integrity and optimizing the organization of key-value pairs for efficient access and storage.

### P2P COMMUNICATION PLATFORM

In this work, implemented a decentralized peer to peer chat application using GunJS which is based on the Patricia Merkle tree concept. The project incorporates an authentication and authorization mechanism designed to seamlessly transition users to the chat interface upon successful validation of their credentials. This innovative approach not only eliminates centralization but also harnesses the decentralized nature of available resources. By decentralizing access control, the system optimizes efficiency and enhances security, aligning with contemporary paradigms in network architecture. This advancement underscores a pivotal shift towards decentralized authentication strategies, promising greater resilience and scalability in modern communication frameworks.

## VI. CONCLUSION

In conclusion, the proposed solution presents a visionary response to the shortcomings of current centralized chat applications in the Web 2.0 era. By leveraging the tenets of Web 3.0 and harnessing the capabilities of blockchain technology, the decentralized chat application not only addresses security concerns but also pioneers a user-centric, trustless environment. The shift away from traditional smart contracts to the innovative use of Patricia Merkle trees signifies a commitment to scalability, efficiency, and adaptability.

This decentralized paradigm ensures that users maintain control and ownership of their data, eliminating the risks associated with a single point of control. The proposed solution stands as a beacon of change in the digital communication landscape, offering a robust, transparent, and tamper-resistant framework. As we embrace this transformative era, the decentralized chat application based on Web 3.0 principles stands as a testament to the endless possibilities of secure and user-centric digital communication.

## VII. FUTURE ENHANCEMENT

Future Enhancements for this decentralized chat application can further solidify its position as a leader in secure and user-centric digital communication. Here are some potential avenues for development:Interoperability with other platforms through well-developed APIs can ensure seamless cross-platform messaging while preserving security and decentralization principles. Improving user experience with intuitive design and responsive support will promote broader adoption. Incorporating advanced cryptographic techniques, such as quantum-resistant algorithms, can safeguard against emerging security threats, ensuring long-term data integrity and user trust. Exploring scalability solutions like sharding or off-chain transactions will help maintain efficiency under heavy usage. Enhanced privacy features, including customizable encryption options and ephemeral messaging, can cater to diverse user preferences. Implementing decentralized identity management will bolster user verification processes and give users greater control over their information. Establishing a community governance model allows users to vote on changes, aligning development with user needs and fostering a sense of ownership. Integrating decentralized finance (DeFi) services within the app can enable new financial interactions, such as peer-to-peer payments and smart contract-based agreements. Incorporating AI and machine learning, while respecting privacy, can enhance functionalities like spam detection and personalized user experiences. Lastly, providing educational resources and support for new users can facilitate smoother onboarding and broader acceptance of decentralized technologies. These enhancements will ensure the application remains at the forefront of secure digital communication in the Web 3.0 era.

## Acknowledgement

I would like to express my sincere gratitude to the anonymous referees whose incisive critiques and helpful suggestions made this article much better. Additionally, I would like to sincerely thank our research domain & work that was supported by the Research and Development (R & D) experts at our college Sri Manakula Vinayagar Engineering College and by our mentor, an expert in Block chain of our department. The direction and thoroughness of this paper have been greatly influenced by their knowledge and mentoring.

## REFERENCES

1. Léo Besançon; Catarina Ferreira Da Silva; Parisa Ghodous; Jean-Patrick Gelas, A Blockchain Ontology for DApps Development, Vol 10, 2022 ,Pg 49905 - 49933, DOI: 10.1109/ACCESS.2022.3173313, IEEE.
2. Peilin Zheng; Zigui Jiang; Jiajing Wu; Zibin Zheng, Blockchain-Based Decentralized Application: A Survey, Vol 4, 2023 ,Pg 121 - 133 , DOI: 10.1109/OJCS.2023.3251854 , IEEE.
3. Siyu Zhu; Cheng Chi; Yang Liu, A study on the challenges and solutions of blockchain interoperability, Vol 20, Iss No: 6 , 2023, Pg 148 - 165, DOI: 10.23919/JCC.2023.00.026 ,IEEE.
4. K. S. Kumar, S. Shaik, and N. G. R. Vullam, Block Chain and Cryptography based Secure Communication System, AJRCoS, vol. 15,Iss no. 3, pp. 40–46, Apr. 2023.
5. Daniel Mawunyo Doe; Jing Li; Niyato Dusit; Zhen Gao; Jun Li; Zhu Han, Promoting the Sustainability of Blockchain in Web 3.0 and the Metaverse Through Diversified Incentive Mechanism Design, 2023
6. Ramazan Yetis; Ozgur Koray Sahingoz, Blockchain Based Secure Communication for IoT Devices in Smart Cities, Vol 7, 2019, Pg 134-138, DOI: 10.1109/SGCF.2019.8782285
7. Debarnab Mitra; Lev Tauz; Lara Dolecek, Graph Coded Merkle Tree: Mitigating Data Availability Attacks in Blockchain Systems Using Informed Design of Polar Factor Graphs, Vol 4, 2023, Pg 434 - 452, DOI:10.1109/JSAIT.2023.3315148, IEEE.
8. Viddi Mardiansyah; Abdul Muis; Riri Fitri Sari, Multi-State Merkle Patricia Trie (MSMPT): High-Performance Data Structures for Multi-Query Processing Based on Lightweight Blockchain, Vol 11, 2023, Pg 117282 - 117296, DOI: 10.1109/ACCESS.2023.3325748, IEEE.
9. Kiseok Jeon; Junghee Lee; Bumsoo Kim; James J. Kim, Hardware Accelerated Reusable Merkle Tree Generation for Bitcoin Blockchain Headers, Vol 22, Iss No 2, 2023, Pg 69 - 72, DOI: 10.1109/LCA.2023.3289515, IEEE.
10. Zhenpeng Liu; Lele Ren; Yongjiang Feng; Shuo Wang; Jianhang Wei, Data Integrity Audit Scheme Based on Quad Merkle Tree and Blockchain, Vol 11, 2023, Pg 59263 - 59273, DOI: 10.1109/ACCESS.2023.3240066, IEEE.
11. Matteo Loporchio; Anna Bernasconi; Damiano Di Francesco Maesa; Laura Ricci, Authenticating Spatial Queries on Blockchain Systems, Vol 9, 2021, Pg 163363 - 163378, DOI: 10.1109/ACCESS.2021.3132990, IEEE
12. Kristof Jannes; Bert Lagaisse; Wouter Joosen, OWebSync: Seamless Synchronization of Distributed Web Clients, Vol 32, Iss No 9, 2021,Pg 2338 - 2351, DOI: 10.1109/TPDS.2021.3066276, IEEE.
13. Teasung Kim; Sejong Lee; Yongseok Kwon; Jaewon Noh; Soohyeong Kim; Sunghyun Cho, SELCOM: Selective Compression Scheme for Lightweight Nodes in Blockchain System, Vol 8, 2020, Pg 225613 - 225626, DOI: 10.1109/ACCESS.2020.3044991, IEEE.
14. Kaifeng Yue; Yuanyuan Zhang; Yanru Chen; Yang Li; Lian Zhao; Chunming Rong; Liangyin Chen, A Survey of Decentralizing Applications via Blockchain: The 5G and Beyond Perspective, Vol 23, Iss No 4, 2021, Pg 2191 2217, DOI: 10.1109/COMST.2021.3115797, IEEE.
15. Zijian Bao; Min Luo; Huaqun Wang; Kim-Kwang Raymond Choo; Debiao He, Blockchain-Based Secure Communication for Space Information Networks,Vol35,Iss,No4,2021,Pg50-57,DOI: 10.1109/MNET.011.2100048, IEEE.
16. Ali Hussain Khan; Naveed Ul Hassan; Chau Yuen; Jun Zhao; Dusit Niyato; Yan Zhang; H. Vincent Poor, Blockchain and 6G: The Future of Secure and Ubiquitous Communication, Vol 29, Iss No 1, 2021, Pg 194 - 201, DOI: 10.1109/MWC.001.2100255, IEEE.
17. Bin Cao; Zixin Wang; Long Zhang; Daquan Feng; Mugen Peng; Lei Zhang; Zhu Han, Blockchain Systems,Technologies,and Applications:A Methodology Perspective, Vol 25, Iss No 1, 2022, Pg353,385,DOI:10.1109/COMST.2022.3204702, IEEE.
18. Tiantong Wu; Guillaume Jourjon; Kanchana Thilakarathna; Phee Lep Yeoh, MapChain-D: A Distributed Blockchain for IIoT Data Storage and Communications, Vol 19, Iss No 9, 2023, Pg 9766 - 9776, DOI: 10.1109/TII.2023.3234631, IEEE.
19. Mahalingam Ramkumar, A blockchain based framework for information system integrity, Vol 16, Iss No 6, 2019, Pg 1 - 17, DOI: 10.23919/JCC.2019.06.001, IEEE.
20. Debashis Das; Sourav Banerjee; Pushpita Chatterjee; Uttam Ghosh; Utpal Biswas, A Secure Blockchain Enabled V2V Communication System Using Smart Contracts, Vol 24, Iss No 4, 2022, Pg 4651 - 4660, DOI:10.1109/TITS.2022.3226626, IEEE.