International Journal of Contemporary Issues in Social Sciences
Volume 3, Issue 3, 2024 ISSN(P):2959-3808 | 2959-2461

A BLOCKCHAIN-BASED IPFS AUGMENTED DISTRIBUTED INFORMATION SHARING PARADIGM FOR SECURE COMMUNICATION IN NETWORKED ENVIRONMENT

Muqadsa Jabeen[*1], **Majid Hussain**[2], **Rana Hassam Ahmed**[3], **Hassan Abbas**[3]

[*1,2,3,4]Dept of Computer Science, The University of Faisalabad, Faisalabad, Pakistan

[*1]muqadsajabeen62@gmail.com; [2]majidhussain1976@gmail.com; [3]ranahassam104@gmail.com; [4]hrabbas7@gmail.com

Corresponding Author: *

Received: July 10, 2024 **Revised:** August 10, 2024 **Accepted:** August 25, 2024 **Published:** September 05, 2024

ABSTRACT

The challenges raised are directly proportional to the progress in data security and information technology. Data sharing, either for internal purposes or across organizations, becomes ever-challenging from the point of view of security. Security aspects are the main problems faced by organizations while communicating data. In spite of the traditional centralized communication systems, there is no answer for the implementation to ensure complete security and privacy. This paper suggests making a truly decentralized communication system for the purpose of sharing information. The aim of this paper is to improve the security and transparency of communication networks using IPFS and blockchain technology, particularly in the aspect of smart contracts. Though the use of blockchain technology is now prevalent in current communication systems, an entirely decentralized messaging network does not exist yet. Communication in the proposed system achieves better cost and latency, with more information shared in real-time without latency. In that system, IPFS, known for its secure and global peer-to-peer (P2P) network, is integrated with the blockchain to allow direct file sharing. We developed this solution in combination with the Ethereum platform and the Solidity programming language.

Keywords: Blockchain, IPFS, Security and privacy, Decentralized, Distributed, Communication Environment, Information Sharing, Smart Contract.

INTRODUCTION

Currently, the growing trend of communication, as an inevitable and important aspect of human life, has led to the emergence of digital communication. The world of communication in ultramodern life allows people to store and collect large quantities of data, performing in attracting a great deal of attention from numerous governments, departments, central systems, and the suchlike. still, world powers have controlled the tremendous power of storehouse in moment's world [1]. On the other hand, the security of particular and organizational information is of great significance in this period. Nonetheless, the results suggested to establish security lack sufficient transparent and are substantially concentrated, indicating the lack of sufficient security. The use of decentralized systems can be a safe, transparent, and suitable result, among which blockchain technology, as a promising strategy, is regarded as one of the most important ways in decentralized systems. Blockchain technology provides the possibility for druggies to duly and fully control their digital individualities and carry out their deals in a secure, transparent, and safe way. Blockchain technology-grounded communication systems profit from asymmetric cryptography, agreement- grounded algorithms, and peer- to- peer network structure [2]. There are presently numerous communication structures) and runner software's that use blockchain technology; But if we examine them, we will see that they either do n't have the complete comprehensiveness for data exchange between sender and receiver as a data exchange system, or if they're comprehensive, they've surely used centralized structures in one or further sections. This will beget some druggies to mistrust them. This exploration seeks to introduce a fully decentralized communication system which is grounded on blockchain technology and utilizes encryption and IPFS technology. Simorgh is a comprehensive data exchange system that has all the features of a communication structure used for data exchange [3].

These centralized networks are unable to provide seamless, instantaneous, secure, or reliable interaction. With the use of blockchain technology, developers may create trustworthy and open decentralized communication networks. Although Blockchain technology is widely employed in existing communication systems, no one has yet created a truly decentralized network for sending and receiving messages. We need a decentralized and safe communication and data exchange mode to realize our vision of a distributed network for sharing information. Several blockchain-based infrastructures are also readily accessible. But if we look closely, they either lack total completeness for data transmission between sender to receiver as a data transfer system or are comprehensive. They have employed central structures in some parts of the system. Some of their users will begin to doubt them due to this. With blockchain, encryption, and the Inter Planetary File System (IPFS), this study aspires to usher in a completely decentralized means of communication. All the components of a communication structure designed for data sharing are included in the suggested system, making it a complete system for exchanging data [4].

Data security and information technology are two areas where problems are increasing in tandem with progress. It is difficult for an organization to communicate data for internal or external communication. Mostly communication systems work in a centralized way where security and privacy issues occur Security and privacy concerns are at odds with the decentralized nature of most communication networks.

1. How Blockchain and IPFS Interact?
2. How to develop a secure data exchange network using Blockchain and IPFS?
3. Which Blockchain platform is used to optimize latency and cost?

The objective of this research is to investigate

- To enable a secure and decentralized data exchange network using blockchain and a decentralized database system.
- To accomplish communication in a decentralized environment between the sender and receiver.
- To optimize latency and cost during communication.

Main Contributions

- Providing consumers with a transparent, secure open-source communication infrastructure that can enable continuous contact.
- Organization-to-organization message transfer without a centralized data server.
- Establishing a network where users can communicate continuously, securely, conveniently, and simply from one organization to another organization.
- utilizing smart contracts to establish the conditions of use for a message from sender to receiver.
- Provide a decentralized secure communication from sender to receiver.

Literature Review

This chapter describes the opportunity of using blockchain technology to decentralize the exchange data network in the centralized communication system. Some works have been done on a decentralized and secure communication basis on a different framework. The creation of decentralized communication systems is currently one of the most important demands in the world. The system's capabilities in comparison to those of other software and hardware were limited to being a sharing files system that was used to protect other blockchain-based systems but had no utility for peer-to-peer communication.

But proper nobody introduced a completely decentralized safe communication system for sender and receiver. Outcomes, this literature is presented on present and current blockchain and IPFS protocols based on sharing and exchanging the data in decentralized. Therefore, we have supposed to create a secure decentralized communication system based on blockchain and IPFS [5].

This paper addresses the concentration of power in centralized web-based platforms and the limitations of decentralized initiatives in providing data owners with control over their data. The authors propose a new source governance context, called ReGov, that enables custom control in decentralized web environments. The framework associations blockchain and reliable implementation surroundings to improve compliance with usage conditions. The effectiveness of ReGov is demonstrated through a thorough study of requirements from a data market state and an assessment of its Privacy, security, and affordability characteristics. The goal is to extend the present state of the art and provide a more comprehensive solution for data ownership and control in decentralized web environments [6].

The author said that technology offers a highly secure and efficient way to store this sensitive information. This study proposes a hyper ledger-based system to track media files as proof in criminal proceedings using a low-cost encrypted blockchain and IPFS. The system restricts user access, prioritizes security, privacy, and authorization, and provides an immutable record of all transactions.The usage of IPFS and hyper ledger provides consistency and sensitivity, and the suggested solution is safer, more immutable, and dependable than alternative systems. Given that Ethereum is an open-source blockchain and does not have the requisite privacy and security characteristics, Hyperledger is thought to be the best platform for criminal record databases. Overall, this study provides a viable response to the difficulties of securely and effectively digitizing criminal data [7].

This author presented methodical works of blockchain-based requests in smart city governance. The review analyzes use cases from seventy-nine selected papers and organizes them using a component-based analysis. The findings indicate that blockchain smart cities is an emerging research area, but more empirical studies using advanced research conventions are needed to spread the maturity of this field. The paper offers a starting position to discuss standards and a reference architecture for a blockchain smart city model and suggests that the secure and scalable infrastructure for blockchain smart cities can be used as a test field for the large-scale adoption of distributed smart city applications. However, the limitation of the study is that it is based on theoretical use cases with limited availability of empirical data [8].

The author proposed Simorgh, a wholly secure and distributed system based on technology of blackchin for share the data in communication systems. The paper argues that current centralized systems cannot suggestion finally clear, dependable, fast, and uninterrupted communication. Simorgh uses IPFS technology to reduce some of the margins of save file and offers privacy, integrity, and accessibility as security features. Simorgh is the very first entirely decentralized messaging system in which node, message, and data storage authentication are all totally decentralized. The paper suggests that Simorgh can be customized for use. It can be used to solve numerous issues and improve the creation of constructions in today's society, as well as in many disciplines and businesses. The paper concludes that Simorgh is the first structure designed to overthrow the centralization of management in the world [9].

This paper proposes a novel approach for decentralized confirmation and circulation of data using blockchain-based attestations in combination with distributed proprieties such as IPFS and Git. The approach goals are to address the scalability problems of blockchains and support multi-protocol storage. A prototypical implementation on the Ethereum blockchain with IPFS and Git was positively evaluated for technical feasibility, with constant transaction sizes and moderate cost and completion time. Future research will explore the delay of the approach to other blockchain platforms andpossibility of processing stored data with blockchain-based processes [10].

A platform for data sharing based on a distributed ledger and Interplanetary File System (IPFS) technologies hybrid was proposed by this researcher. Data sharing is being challenged by the rapid growth of data interchange as a result of the information age's ongoing development. The suggested system intends to address this issue by constructing the IPFS storage system, which makes use of shared storage, file dividing and cutting, redundancy backup, and other technologies, as well as a consensus process of computer power competition to keep the data on the blockchain. The system is made up of a datasharing platform with four modules: a quick retrieval module, an IPFS module, a blockchain module, and an “encryption and decryption module”. The created data is encrypted using the AES encryption technique, and after it's uploaded to the IPFS system, it is broken up and stored using distributed storage technology. Through the blockchain element, the intellectual and other data are eventually written into the blockchain, and the extraordinary recovery modules can quickly find the necessary data in the huge blockchain data due to the retrieval conditions. The suggested method offers guidance for the secure preservation and storage of data. The system resolves the issue of extensive data sharing, realizes data decentralization, and assures the security of data storage by developing a network with blockchain and IPFS technology [11].

This research proposed a novel blockchain-based secure decentralized system for data transfer and access control in cloud servers using IPFS. The system aims to address the security issues related to centralized systems, where the data can be manipulated by internal personnel and suffer from a “single point of failure”. In the suggested method, the information's user uploads a file with encryption to IPFS, it is then divided for data protection into n discrete parts called hash codes. The system employs two-level key management, in which the file's owner first encrypts it before the IPFS server generates a hash of it. The blockchain-based system enables consumers to be dealt with across multiple domains, removes the single point of failure in traditional centralized systems, and reduces overhead associated with communication and calculation at the consumer level. The user authorizations are written as well by the information owner to achieve access to this secure data. Additionally, the system may create reliable, unchangeable access logs that make it simple for data owners to later track users' access activities. The cost of downloading data at the user's level is quite minimal, according to experiments. Due to the blockchain's capacity to generate a original hash code for altered data each period it is altered, the initial information on a decentralized network cannot be altered by any other users or members. Decentralized rather than centralized data access is, therefore, more secure. The security research found that the suggested solution could effectively fend off malicious users both individually and collectively, as well as unreliable cloud servers [12].

The author presented a blockchain-based confidentiality records of data exchanged scheme for smart factories in the Industrial Internet of Things (IIoT) to improve the accuracy of equipment fault detection and reduce losses caused by low fault recognition rates. The scheme is based on the abstraction of smart industrial as edge nodes and the use of decentralized, distributed blockchain networks built on Ethereum clients. A reputationbased Delegated Proof of Stake (RDPoS) consensus algorithm, an incentive mechanism based on data characteristics to encourage nodes at the edge to communicate data, and an Intelligent Elliptic Curve Digital Signature Algorithm (IECDSA) to ensure that shared information is owned by edge nodes are all part of the proposed solution. The proposed technique increases edge nodes' eagerness to share data while ensuring its security, as shown by the authors' theoretical and simulated studies. The suggested blockchain-based private information security sharing system has a four-step workflow: verifying the data that is to be communicated and saving it in the blockchain technology, sharing the information across edge devices, and finally publishing the information.The proposed method was evaluated using VMware Workstation, but the authors advise that in the future, testing the approaches on actual local area networks and using game theory to enhance the incentive mechanism may be done [13].

According to the researcher, the present cloud-based system enabling IoT information preservation, processing, and sharing mainly depends on an established independent auditor (TPA) and operates under centralized supervision, which may lead to serious data leakage and compromise user privacy. This paper suggests a decentralized distributed file storage and data exchanging system created on blockchain technology to address this issue. This system offers secure encryption throughout and limited access based on access control determined by attributes (A-BAC) policy. The proposed model, named IoT Chain, offers the Ethereum distributed ledger and the interplanetary file system (IPFS) Experimental results show that the proposed system provides robust, comprehensive, and secure storage services, and the scheme is logical and frugal in design [14].

The author addressed the trials challenged in the adoption and utilization of Blockchain technology by various stakeholders, such as SMEs, companies, organizations, businesses, government institutions, and the general public. The main challenges discussed are cybersecurity and data privacy. The paper highlights the need for investment and research in these areas to ensure that the public and private areas have trust in the technology. A framework is proposed that incorporates elements of Big Data, Machine Learning, and Visualization to experiment with data processing and storage securely and transparently [15].

This author suggested a decentralized IIoT system that makes use of IPFS and smart contracts on Ethereum for efficient and safe data storage. By leveraging smart contract technology for device authentication and IPFS for distributed data storage, the solution does away with the necessity for a Verified Third Party and addresses problems like

“Single-Point-of-Failure”, trust concerns, privacy and security. The suggested system has been constructed and tested in test networks using JavaScript VM and rotten, and it also contains data accessing regulations for end users. The simulation's findings, which included expenses that were estimated and compared to recent research, demonstrated that the infrastructure is safe and satisfies important security requirements [16].

The author addressed the difficulty of copyright infringement in the sharing of multimedia content online and proposes a solution using a distributed P2P video and image, audio exchange platform built on blockchain technology and IPFS. The approach uses perceptual hash (pHash) to detect copyright violations, which allows for the identification of tampered multimedia content. The procedure of blockchain technology provides a noninvolvement of third parties and avoids single points of failure. Copyright violation is a significant challenge in the digital age, and the proposed approach offers a potential solution to the difficult [17].

File Share, a decentralized program system for transferring files and data provenance, was introduced by the author. It addresses integrity and ownership issues by utilizing Ethereum smart contracts and IPFS, a distributed file system. The application allows users to create and store files securely, and access them only through the inbuilt editor. The blockchain network gathers and stores provenance data, enabling visibility and tracking into the past of shared content. User registration and verification, creating files and storing spaces. file retrieving and origin data gathering and storage are the framework's four core phases. In a file system that is distributed, the program offers a tamper-proof paradigm for file sharing, and the history of data can be applied for analytical reasons [18].

This author presented a model of covert communication that uses smart contracts in a blockchain environment to securely transfer information. Traditional communication channels using a “third-party” node are exposed to attacks and data tampering, and identity information is not always secure. Smart contracts, with their decentralization and tamperresistant characteristics, can offer a solution to these problems.The authors provide an information-transfer model for clandestine communication that makes use of smart contracts. To guarantee data privacy and security, the suggested paradigm makes use of two-round protocols and encryption methods. The model is optimized to reduce costs and increase concealment. The authors use voting and secret bidding contracts as examples to describe the proposed method. The process of covert communication is distributed into seven parts, including data processing, keyword extraction, keyword delivery, contract generation, contract invocation, information extraction, and inverse processing of information. The authors provide new results that show the proposed model is tamperresistant and feasible for covert communication [19].

The researcher discussed the need for an advanced degree of safety and truth in the current web-based environment, which is accessed by smart gadgets. It highlights the vulnerabilities associated with the old web-based applications deployed on central servers and the need for decentralized cloud integrations to secure services like E-Governance. The article emphasizes the role of blockchain technology in providing a secure and decentralized environment by using cryptographic principles to protect data nodes and connect them.Additionally, it emphasizes IPFS's capabilities as a cutting-edge technology for a secure blockchain environment. The essay concludes with a discussion of the advantages of a decentralized internet when applications and information are kept across several locations using the technology of blockchain to assure security and privacy [20].

The researcher presented a secure data-sharing mechanism based on blockchain for Vehicular Networks (VNs) that uses advantage facility available and a circulated file storage system to efficiently manage service provisioning and tackle issues related to centralized architectures. Economic motivations are specified to edge vehicle nodes, and smart contracts automate system processes, whereas the system is improved by the inclusion of a Authority of proof consensus mechanism [26]. A symmetric keys cryptographic approach that also improves security and privacy determines the reputation values of nodes according to their trust values. The proposed system is efficient for VNs, and future work will focus on fake review detection systems and algorithms to balance system cost and data size [21].

This author identified the solution a secure file-sharing system based on the combination of Inter-Planetary File System (IPFS) and blockchain technologies. Although blockchain is good at recording transactions, IPFS is used for storing large files or documents in a decentralized way. The files encrypted by the IPFS proxy can be saved on the IPFS server, and the suggested system exploits an IPFS gateway for decentralized permissions and group key management. Blockchain is utilized as a traceable server to log information about file uploads and prevent data corruption. In an encrypted structure, where users may establish or enter organizations and access only approved files, IPFS and blockchain are combined using the IPFS proxy. The paper presents a solution to overcome the limitations of previous schemes and enhance security and computation overheads [22]. This author proposed a blockchain-based solution using Ethereum smart contracts, IPFS and trusted oracles for managing patient health records (PHRs) in a decentralized, traceable, reliable, trustful, and safe manner [27]. The proposed solution addresses the limitations of current centralized PHR management systems by giving patients control over their medical data. The paper presents algorithms and implementation details, evaluates the proposed contracts using cost and correctness metrics, and provides security analysis. The paper outlines the limits of the planned method, such as interoperability, key management, GDPR, and smart contract upgradability.Despite these drawbacks, the suggested technique is universal and may be applied to blockchain networks with or without authorization [23]. This author discussed the possible benefits and trials of implementing blockchain technology in governmental processes, specifically in the e-government areas. The authors argue that a need-driven approach should be taken, where managerial procedures are altered to fit the technology rather than the other way around [28]. They also stress the importance of sound governance models to ensure the realization of benefits. The author presented two perspectives for governments concerning blockchain technology: governance by blockchain, where public organizations accept blockchain technology for their processes, and governance of blockchain, which determines how blockchain should be designed and used to fulfill public values and social needs. The authors note that implementing blockchain technology in e-government requires experimentation and exploration of possible applications to avoid costly failures table no 2 is shown comparison literature [24].

The authors also highlighted the challenges of designing for flexibility in blockchain systems while maintaining the technology's built-in mechanisms for consensus and continuance. They call for further research into changes in data stewardship and responsibility roles, trust creation, governance models, and the effects of blockchain technology on organizational transformation and auditing.The author talked about some of the limitations of blockchain technology, such as how expensive storage is and how difficult it is to store massive volumes of information on the blockchain technology. These issues can be avoided using cryptographic hashes, and IPFS uses a special method to save passwords to files on the ledger that is distributed rather than the real files themselves. Such hashes can be used to find the file's true location, and by using cryptography's public and private keys, specific people can be granted access [25].

Proposed Methodology

In this thesis, I have proposed a decentralized secure communication system for a sender to receiver in an organization show Error! Reference source not found.

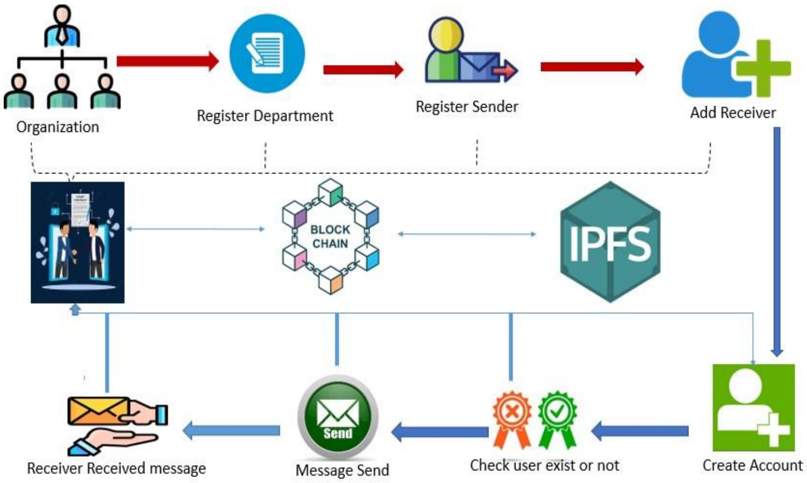


Figure 1: Proposed Model Organizational Sender to Receiver message Transfer

In this section, we proposed a blockchain-based model to secure communication for an organization. We used the Ethereum platform.a blockchain platform that facilitates the development of decentralized applications (dapps) and smart contracts. Its cryptocurrency is ether, is also available. A decentralized blockchain with smart contract capabilities is called Ethereum. We used solidity language in remix ide. In this Proposed Model Figure 1 explains the sender-to-receiver communication in the organization. Firstly, one organization will register the department for communication with other organizations. For security senders will register themselves in any organization. After registration, the sender will be sent a message to another organization where it will be verifying whether the user exists or not. After its verification, the sender can talk and send the message to a second person to whom the receiver will have received the message. It is a decentralized proposed model in that every node is connected to another.

Tool and Techniques

Ethereum

I chose the Ethereum platform for my research. Ethereum is a peer-to-peer blockchain technology that enables safe smart contract programme execution and certification. Smart contracts do away with the need for a reliable centralized entity so that parties can deal with one another directly. Participants have total visibility and control over transactionrelateddata since records of transactions are unchanging, verifiable, and securely sent throughout the network.Transactions can be sent and received using user-created Ethereum accounts. The sender is required to sign messages and utilize Ether, Ethereum's native currency, as a price for carrying out activities on the network.

Remix Ide

For the Ethereum blockchain network, Remix is an Integrated Development Environment (IDE) that is web-based. It provides a simple interface for Writing, Testing, and Deploying smart contracts written in Solidity, the programming language used to develop applications on the Ethereum platform. With Remix, developers can quickly write and deploy smart contracts, test them with sample data, and debug any errors. Additionally, Remix provides a user-friendly interface for executing smart contract functions and viewing the transaction history. Overall, Remix is a valuable tool for Ethereum developers who want to streamline their workflow and create applications on the Ethereum platform.

Metamask

A simple user interface for dealing with decentralized apps (dApps) developed on the Ethereum blockchain is provided by MetaMask, a browser extension. It permits users to strongly store and accomplish their Ethereum addresses, as well as to send and receive Ether and other Ethereum-based assets.

With MetaMask, users can interact with dApps directly from their browsers without having to run a full Ethereum node. This makes it much easier for users to participate in decentralized applications, as they can access them from anywhere and do not have to worry about the technical details of setting up a node.

MetaMask also serves as a bridge between the Ethereum network and the user's browser, enabling users to sign transactions and access their Ethereum accounts without exposing their private keys. This helps ensure the security of users' assets and personal information. MetaMask is a popular and widely used tool for accessing and interacting with the Ethereum blockchain and its decentralized applications.

Georli Testing Networks:

Metamask is a popular browser extension that provides a user-friendly interface for interacting with blockchain networks, including Ethereum and its test networks such as Goerli.

In the context of the Goerli network, Metamask can be used to connect to the network and interact with test Ethereum tokens, test smart contracts, and dapps. To connect Metamask to the Goerli network, users need to switch the network from the main net to Goerli in the Metamask interface.

Once connected to the Goerli network, users can perform various tasks such as sending and receiving test Ethereum tokens, interacting with test smart contracts, and testing dapps. As a result, programmers can test their applications in a safe location before launching them on the Ethereum main net. Metamask can also be used to manage and store Ethereum and ERC-20 tokens on the Goerli network. Users can add custom tokens to their Metamask wallets by providing the token's contract address, symbol, and decimal places.

Metamask is a useful tool for interacting with the Goerli network, as it provides a userfriendly interface and allows for easy testing of smart contracts and dapps.

Solidity:

Solidity is a programming language that is utilized by the Ethereum blockchain to build smart contracts. Smart contracts is also known as self-executing programs that autonomously enforce the terms of a contract between two parties without the use of middlemen.It is high-level, object-oriented programming language created expressly for smart contracts is called Solidity. It is user-defined typed, allows inheritance, and libraries, and is statically typed, which means a variable's type must be stated before it is used. Decentralized applications (dapps) are developed largely using Solidity and run on the Ethereum network. Dapps are computer programs that are constructed on top of a blockchain network and run on a decentralized system.

Various corporate activities, including financial transactions, supply chain management, and identity verification, can be automated using smart contracts created in Solidity. Solidity enables programmers to construct intricate business logic and build safe, intermediary-free systems.For developers looking to create decentralized applications on the Ethereum blockchain, Solidity is a potent tool. Its connection with the Ethereum Virtual Machine (EVM) enables secure, decentralized implementation of smart contracts, and its high-level, object-oriented syntax makes it simple to learn for developers with prior experience in other programming languages.

Optimize the Smart Contract GAS:

Gas units used by smart contracts are used to compute the system cost consumption. The processing power required for the execution of transactions on the Ethereum platform is measured in units called "gas." The miners set the petrol price at the beginning of the transaction, and it is expressed in Gwei. Additionally, gas units are computed to carry out smart contracts' functions. Gas units are transformed into ether value, often known as fiat money, in the Ethereum blockchain. The Ethereum blockchain runs on ETH. The value of eth is created using the gas units. A 20 Gwei petrol surcharge has been introduced. Additionally, the price of Gwei is determined by multiplying petrol units by the price of petrol. The sum is then divided by one ether, which is equal to 1,000,000,000 Gwei, to determine the amount. Cost of transaction: It represents the price of transferring the code for smart contracts to the Ethereum blockchain.

Transaction Fee: (Gas consumed * Gas Price) *(Ether price/ 10^9)

The size of the smart contract determines this. The computational tasks a smart contract handles determine its size. For instance, if a smart contract has many computing activities, it will be enormous and have a high transaction cost. Additionally, the transaction cost is made up of the following costs: transaction, contract deployment, and transaction data. Cost of execution: It is the price of keeping global variables and smart contract method calls. In the context of transaction execution, it additionally depends on the mathematical procedures carried out. Gas cost, gas cost, and gas limit are the three factors used to compute the gas. The quantity of units required to carry out any action on the Ethereum network is known as the gas cost. The price of petrol is expressed as the value of one ether unit. The gas limitation is the total quantity of gas that network users must pay. Developers encounter a recurring problem as Ethereum maintains its popularity due to its adaptability and capacity to handle DApps and smart contracts. Gas consumed by the organization was 158760, and the cost of execution was 138852.Gas table 1 presented here.

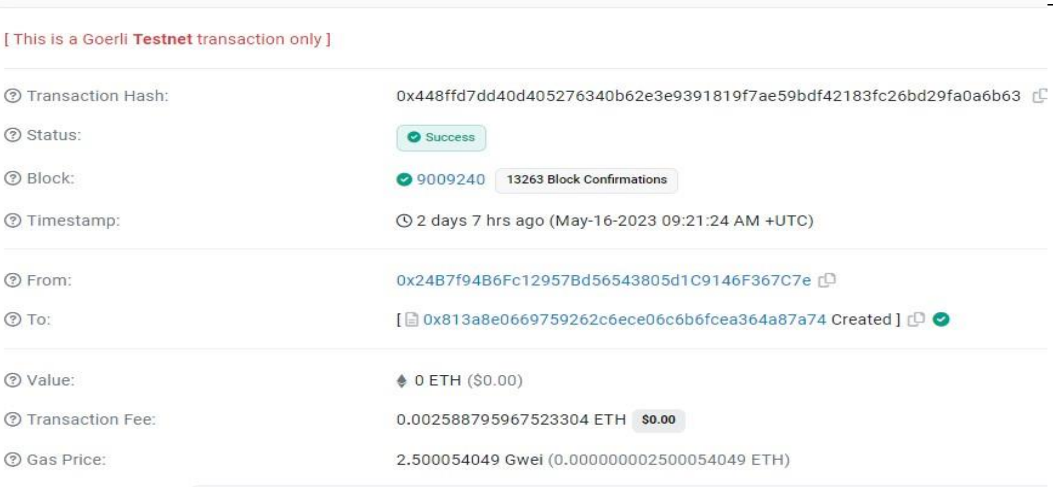
Table No 1: Used Function with their Gas

Operation	**Gas**	**Description**
Add, Sub	3	Arithmetic Operation
Multiply, Divide	5	Arithmetic Operation
Pop	2	Stack Operation
Push, Dup, Swap	3	Stack Operation
M load, M store	3	Memory Operation
Jump	8	Unconditional Jump
S Load,	200	Storage Operation
S Store	5,000 20,000	Storage Operation
Call	25,000	Create a new account using call
Create	32,000	Create new account using create
Balance	400	Get balance of an account

Results and Discussion

Experiments and Results Analysis

In this part, to find outcomes and graphs for smart contracts, we use the Remix Ethereum IDE. Because we cannot transact smart contracts or ether without gas, gas is a crucial component of the Ethereum IDE. This figure shows in 2 that the status is successful and already shows the sender and receiver address. This smart contract consumed 2.500054089 ETH. Utilizing Gas Limit * Gas Price Per Unit, the gas fee is determined.1 The computation would result in 20,000 * 200 = 4,000,000 gwei or 0.004 ETH if the petrol cap was set at 20,000 and the cost per unit was 200 gwei.



[This is a Goerli **Testnet** transaction only]

Transaction Hash:	0x448ffd7dd40d405276340b62e3e9391819f7ae59bdf42183fc26bd29fa0a6b63
Status:	Success
Block:	9009240 13263 Block Confirmations
Timestamp:	2 days 7 hrs ago (May-16-2023 09:21:24 AM +UTC)
From:	0x24B7f94B6Fc12957Bd56543805d1C9146F367C7e
To:	[0x813a8e0669759262c6ece06c6b6fcea364a87a74 Created]
Value:	0 ETH ($0.00)
Transaction Fee:	0.002588795967523304 ETH $0.00
Gas Price:	2.500054049 Gwei (0.000000002500054049 ETH)

Figure 2:Gas Optimization

Figure 3 show that status of transaction with their transaction fee, Gas Fee, Gas limit and also show transaction hash value.Blockchain is used as a security because it has a unique hash value.

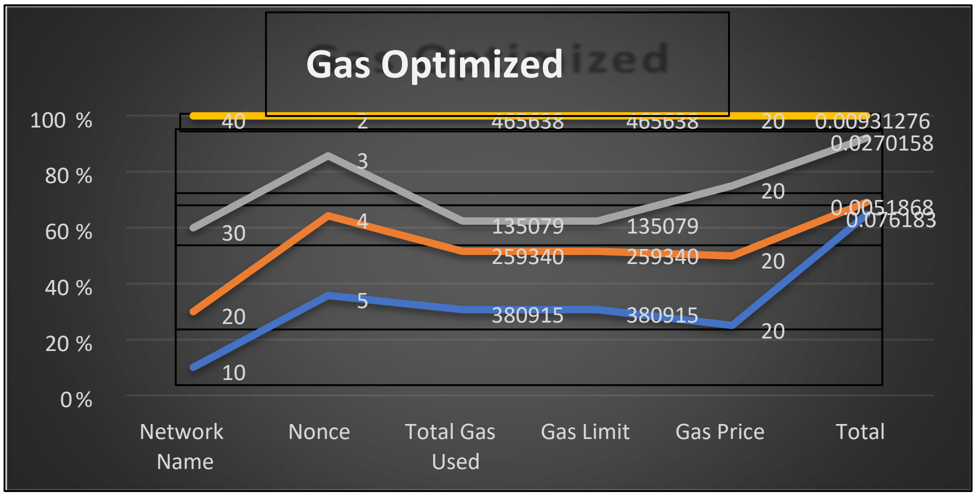
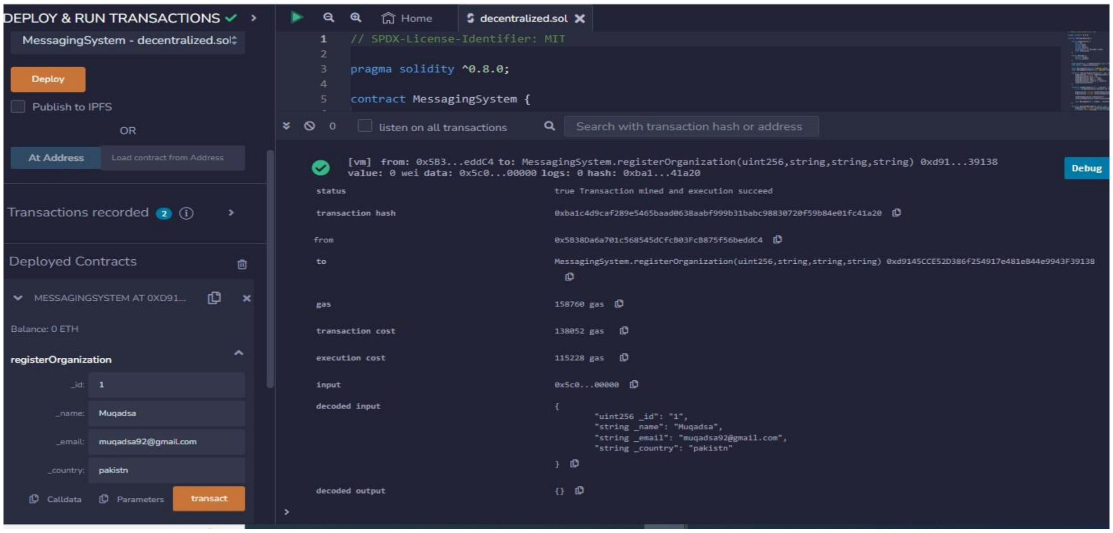


Figure 3:Gas Optimization of Smart Contract



MessagingSystem - decentralized.sol

□ Publish to IPFS

Balance: 0 ETH

registerOrganization

_id: 1
_name: Muqadsa
_email: muqadsa92@gmail.com
_country: pakistn

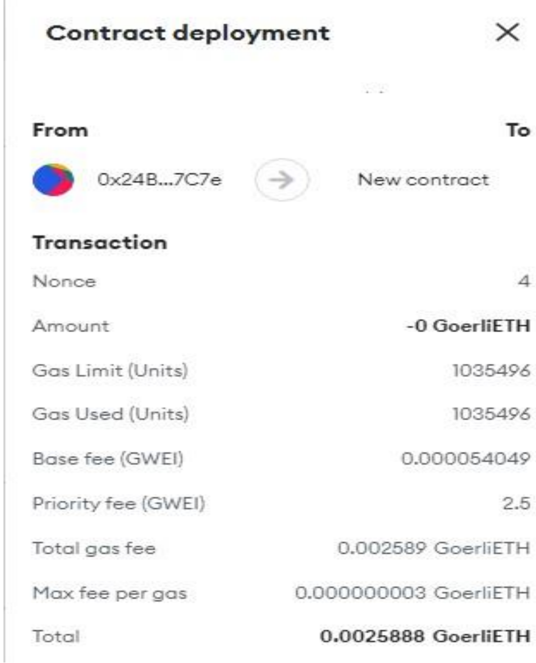
```
// SPDX-License-Identifier: MIT

pragma solidity ^0.8.0;

contract MessagingSystem {
```

0 □ listen on all transactions   Search with transaction hash or address

```
[vm]  from: 0x5B3...eddC4 to: MessagingSystem.registerOrganization(uint256,string,string,string) 0xd91...39138
value: 0 wei data: 0x5c0...00000 logs: 0 hash: 0xba1...41a20
status              true Transaction mined and execution succeed
transaction hash    0xba1c4d9caf289e5465baad0638aabf999b31babc98830720f59b84e01fc41a20
from                0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to                  MessagingSystem.registerOrganization(uint256,string,string,string) 0xd9145CCE52D386f254917e481eB44e9943F39138
gas                 158760 gas
transaction cost    138052 gas
execution cost      115228 gas
input               0x5c0...00000
decoded input       {
                            "uint256 _id": "1",
                            "string _name": "Muqadsa",
                            "string _email": "muqadsa92@gmail.com",
                            "string _country": "pakistn"
                    }
decoded output      {}
>
```

Figure 4:Register Organization

This figure show Figure 4 register organization with their verification organization register.



Contract deployment ✕

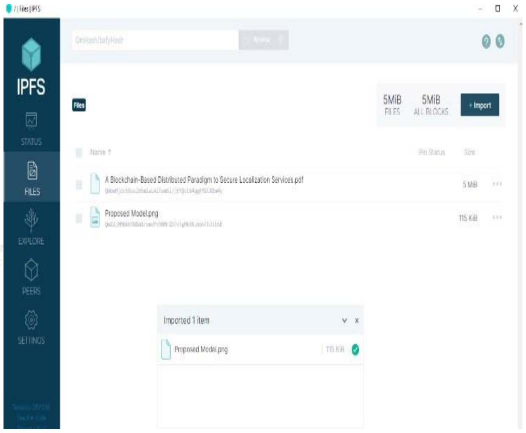
From	To
0x24B...7C7e	New contract

Transaction

Nonce	4
Amount	-0 GoerliETH
Gas Limit (Units)	1035496
Gas Used (Units)	1035496
Base fee (GWEI)	0.000054049
Priority fee (GWEI)	2.5
Total gas fee	0.002589 GoerliETH
Max fee per gas	0.000000003 GoerliETH
Total	0.0025888 GoerliETH

Figure 5: Transaction in MetaMask

This figure shows Figure 5 sender to receiver communication in an organization ad show that total gas and consumed gas in used in smart contract.



5MiB FILES 5MiB ALL BLOCKS

Name	Size
A Blockchain-Based Distributed Paradigm to Secure Localization Services.pdf	5 MiB
Proposed Model.png	115 KiB

Imported 1 item

Proposed Model.png 115 KiB ✓

Figure 6:File and Image upload IPFS

This figure show Figure 6 that IPFS relies on content addressing as its main method of locating and obtaining files from its network. With content addressing, a file's unique identification is obtained from its content rather than from its location or the name given to it. As a result, even within a distributed and decentralized setting, files may be effectively discovered and retrieved. It shows the hash value which is generated by IPFS.

Conclusion

In this thesis, we presented a decentralized communication system for sender to receiver in an organization. This study offers a decentralized system based on Blockchain and IPFS for organizations, which permits numerous organizations to access data from decentralized communication safely. One organization can share data with another organization. Data owner-user agreements are permanently recorded using blockchain technology. The proposed techniques offer data transparency, accountability, Transparent & Uninterrupted. The user will share information without any delinquency. Nowadays, IPFS is considered the best amalgamation with blockchain and is being used because this system permits the user's direct file sharing through a secure and worldwide P2P network. We Optimized the cost and latency to the sender and receiver during communication.

References

Ali, M.A. and Bhaya, W.S., 2020, December. Blockchain technology's applications and challenges: An overview. In *AIP Conference Proceedings* (Vol. 2290, No. 1, p. 040019). AIP Publishing LLC.

Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H., 2017, June. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). Ieee.

Xu, X., Weber, I. and Staples, M., 2019. *Architecture for blockchain applications* (pp. 1307). Cham: Springer.

Ismail, L. and Materwala, H., 2019. A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. *Symmetry*, *11*(10), p.1198.

] Kim, S. and Deka, G.C. eds., 2020. *Advanced applications of blockchain technology*. Berlin/Heidelberg, Germany: Springer.

Zheng, Q., Li, Y., Chen, P. and Dong, X., 2018, December. An innovative IPFS-based storage model for blockchain. In *2018 IEEE/WIC/ACM international conference on web intelligence (WI)* (pp. 704-708). IEEE.

Ahmed, M., Pranta, A.R., Koly, M.F.A., Taher, F. and Khan, M.A., 2023. Using IPFS and Hyperledger on Private Blockchain to Secure the Criminal Record System. *European Journal of Information Technologies and Computer Science*, *3*(1), pp.1-6.

Zygiaris, S., Saleh, M.F. and Al-Imamy, S.Y., 2023, THE SMART CITY BLOCKCHAIN GOVERNANCE: A LITERATURE REVIEW

Mirzaei, E. and Hadian Dehkordi, M., 2022. Simorgh, a fully decentralized blockchainbased secure communication system. *Journal of Ambient Intelligence and Humanized Computing*, pp.1-19.

Härer, F. and Fill, H.G., 2022. Decentralized attestation and distribution of information using blockchains and multi-protocol storage. *IEEE Access*, *10*, pp.18035-18054

Li, W., Zhou, Z., Fan, W. and Gao, J., 2022. Design of Data Sharing Platform Based on
Blockchain and IPFS Technology. *Wireless Communications and Mobile*
Computing, *2022*

Athanere, S. and Thakur, R., 2022. Blockchain-based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing. *Journal of King Saud University-Computer and Information Sciences*, *34*(4), pp.1523-1534.

Wang, Y., Che, T., Zhao, X., Zhou, T., Zhang, K. and Hu, X., 2022. A Blockchain-Based
Privacy Information Security Sharing Scheme in Industrial Internet of
Things. *Sensors*, *22*(9), p.3426

Ullah, Z., Raza, B., Shah, H., Khan, S. and Waheed, A., 2022. Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment. *IEEE Access*, *10*, pp.36978-36994.

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C. and Platts, J., 2022. Cybersecurity, data privacy and blockchain: A review. *SN Computer Science*, *3*(2), p.127.

YILDIZ, B., 2021. Internet of Things and Smart Cities: A Bibliometric Analysis. *Quantrade Journal of Complex Systems in Social Sciences*, *3*(1), pp.27-44.

] Kumar, R., Tripathi, R., Marchang, N., Srivastava, G., Gadekallu, T.R. and Xiong, N.N., 2021. A secured distributed detection system based on IPFS and blockchain for industrial image and video data security. *Journal of Parallel and Distributed Computing*, *152*, pp.128-143.

] Kumar, R., Tripathi, R., Marchang, N., Srivastava, G., Gadekallu, T.R. and Xiong, N.N., 2021. A secured distributed detection system based on IPFS and blockchain for industrial image and video data security. *Journal of Parallel and Distributed Computing*, *152*, pp.128-143

Iqbal, A.,Rajasekaran, A.S., Nikhil, G.S. and Azees, M., 2021. A secure and decentralized blockchain based EV energy trading model using smart contract in V2G network. *IEEE Access*, *9*, pp.75761-75777.

Mendu, M., Krishna, B., Mohmmad, S., Sharvani, Y. and Reddy, C.V.K., 2020, December. Secure deployment of decentralized cloud in blockchain environment using inter-planetary file system. In

IOP Conference Series: Materials Science and Engineering (Vol. 981, No.
2, p. 022037). IOP Publishing.

Javed, M.U., Rehman, M., Javaid, N., Aldegheishem, A., Alrajeh, N. and Tahir, M., 2020. Blockchain-based secure data storage for distributed vehicular networks. *Applied Sciences*, *10*(6), p.2011.

Huang, H.S., Chang, T.S. and Wu, J.Y., 2020, July. A secure file sharing system based on IPFS and blockchain. In *Proceedings of the 2020 2nd International Electronics Communication Conference* (pp. 96-100).

Madine, M.M., Battah, A.A., Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y., Pesic, S. and Ellahham, S., 2020. Blockchain for giving patients control over their medical records. *IEEE Access*, *8*, pp.193102-193115.

Dwivedi, S.K., Amin, R., Vollala, S. and Chaudhry, R., 2020. Blockchain-based secured event-information sharing protocol in internet of vehicles for smart cities. *Computers & Electrical Engineering*, *86*, p.106719.

Vimal, S. and Srivatsa, S.K., 2019. A new cluster P2P file sharing system based on IPFS and blockchain technology. *Journal of Ambient Intelligence and Humanized Computing*, pp.1-7.

Nazir, Talha, et al. "Transforming Blood Donation Processes with Blockchain and IoT Integration: A augmented Approach to Secure and Efficient Healthcare Practices." 2023 International Conference on IT and Industrial Technologies (ICIT). IEEE, 2023.

Abbas, Hassan, et al. "Enhancing Food Security: A Blockchain-Enabled Traceability Framework to Mitigate Stockpiling of Food Commodities." *2023 International Conference on IT and Industrial Technologies (ICIT)*. IEEE, 2023.

Zahid, Samraiz, et al. "Blockchain-based Health Insurance Model Using IPFS: A Solution for Improved Optimization, Trustability, and User Control." *2023 International Conference on IT and Industrial Technologies (ICIT)*. IEEE, 2023.

IJCISS
International Journal of Contemporary Issues in Social Science