Integrating Privacy and Security in Smart Cities: A Blockchain-based IPFS Framework

Ibtisam Ehsan[1,†], Muhammad Irfan Khalid[2,†], Markus Helfert[3,4,†], Nadeem Yaqub[5,†] and Mansoor Ahmed[3,4,*,†]

[1]School of Computer Science and Technology, University of Chinese Academy of Sciences
[2]University of Sialkot, Pakistan
[3]Innovation Value Institute, Maynooth University, Maynooth, Ireland
[4]Adapt Centre for AI-driven Digital Content Technology, Ireland
[5]Beijing University of Technology Beijing, China

Abstract

Smart Cities have been a topic of discussion over the past few years and have made great strides regarding incorporating technologies such as the IoT, blockchain, and cloud computing to enhance the lives of citizens. Among these technologies, the most noteworthy is the blockchain, which serves as an evolving means of accountability for virtual assets in digital currencies such as Bitcoins. To fully harness the potential of blockchain in smart cities, a comprehensive understanding of its features, essential requirements, and research challenges is crucial. Consequently, this article aims to outline the features of blockchain that are suitable for the context of smart cities and determine significant preconditions for its adoption. It presents a new framework that leverages IPFS for smart city security and multiple case studies of designing a smart city using blockchain. The proposed architecture was implemented through simulations and testing, demonstrating how blockchain can be effectively utilized in disaster management. Moreover, the research benchmarked the effectiveness of compensation management and the comparison of gas costs to the changes in the perceived transaction costs. The work also discusses smart contract algorithms for various smart city applications while pointing out the role of trust and acceptance in implementing blockchain solutions. The research is aimed at challenging areas, such as data security and uncovering possible solutions in storage, thus guiding the framework for an integral, safe, and sustainable smart city solution based on the use of blockchain.

Keywords

Smart cities, Blockchain, Security, Privacy-Preserving, IPFS

1. Introduction

Urbanization has profoundly impacted citizens and their quality of life, as evidenced by various statistics from the United Nations[1]. The rapid increase in population density in urban areas has led to numerous challenges, including chronic traffic congestion, waste disposal issues, and heightened pollution levels in both air and water resources. These problems create significant obstacles to the well-being of urban residents, necessitating innovative solutions that can enhance the living conditions in cities. In this context, the concept of smart cities has emerged as a promising approach to tackle these challenges, utilizing advanced information and communication technologies (ICT) to create sustainable living environments that significantly improve the quality of life for inhabitants.

Smart cities are characterized by their use of interconnected technologies that facilitate efficient urban management. Key components of smart city infrastructure include smart database systems that

Companion Proceedings of the 17th IFIP WG 8.1 Working Conference on the Practice of Enterprise Modeling Forum, M4S, FACETE, AEM, Tools and Demos co-located with PoEM 2024, Stockholm, Sweden, December 3-5, 2024
***

[†]These authors contributed equally.

ibtisamehsan146@gmail.com (I. Ehsan); irfanse6235@gmail.com (M. I. Khalid); markus.helfert@mu.ie (M. Helfert); nadeem.yb@gmail.com (N. Yaqub); mansoor.ahmed@mu.ie (M. Ahmed)
0000-0003-1804-8670 (I. Ehsan); 0000-0003-1804-8670 (M. I. Khalid); 0000-0001-6546-6408 (M. Helfert); 0000-0003-2034-1403 (N. Yaqub); 0000-0003-2034-1403 (M. Ahmed)

support the storage and processing of vast amounts of data generated by various urban activities, smart control systems that monitor events and manage urban operations in real time, smart interfaces that provide seamless interaction between citizens and city services, and smart carriers that enhance the logistics of goods and services. The successful assimilation of these elements is crucial for effectively integrating blockchain technology into smart city applications, as each component plays a pivotal role in ensuring the system's overall functionality and resilience[2].

Our research seeks to bridge the gap in the existing literature by identifying the requirements for successful blockchain implementation within smart city frameworks and addressing the key challenges associated with this integration. Specifically, we introduce a comprehensive framework that integrates blockchain technology with the InterPlanetary File System (IPFS), designed to enhance data security and privacy. This framework is particularly relevant in the context of smart cities, where sensitive data from various sources needs to be managed securely and efficiently[3].

Through detailed scenarios and case studies, we demonstrate the effectiveness of our proposed framework, highlighting its ability to improve urban operations across a range of applications, from traffic management to waste collection and environmental monitoring. Furthermore, we provide a comparative analysis that showcases the superior performance of our integrated system in critical attributes such as data integrity, accessibility, and operational efficiency, making it a valuable tool for city planners and administrators.

Additionally, we address the challenges related to scalability and dataset management that may arise during the implementation of blockchain solutions in smart cities. By offering insights into how these challenges can be mitigated, we provide a roadmap for researchers and practitioners looking to adopt blockchain technology in urban contexts[4].

Finally, this study enhances the knowledge of incorporating blockchain and IPFS as our findings highlight potential opportunities and challenges within Smart City components. Organizations primarily focus on efficacy, security, and sustainability when considering the adoption of different structures. Our goal is to ensure appropriate and legitimate data usage, which will enhance the stable foundation necessary for developing smart cities. This effort aims to improve the quality of life for citizens and create environments better equipped to handle the challenges and new demands of urban living.[5].

1.1. Our Contributions

- Introduces a framework integrating blockchain technology with IPFS to enhance data security and privacy in smart cities.
- Demonstrates the framework's effectiveness through detailed scenarios.
- Provides a comparative analysis showing superior performance of the proposed system in attributes.
- Discusses challenges related to scalability and dataset management.
- The implementation of our proposed blockchain smart contracts. and related metadata is publicly available on the following GitHub repository https://github.com/ibtisam-111/Blockchain-Smart-Cities-IPFS

You can check the project code in the GitHub repository to reproduce this research contribution in your environment. Any researcher who wants to take this work forward or construct it can go through the detailed steps documented in the repository.

1.2. Paper Structure

The paper is organized as follows: First, the introduction section proceeds by shedding light on the role of blockchain and IPFS for secure smart cities. The next section presents relevant studies literature. The subsequent sections detail the proposed framework and its application in three key scenarios and their deployment. In the next section, a comparison with other studies is presented. In the last section of the paper, the authors conclude, offering an overview of the mentioned findings and limitations.

2. Background and Related Studies

In recent days, emerging solutions in smart cities have related to the integration of blockchain to improve its reliability and security in recent years. The subsequent sections outline the papers that focus on different aspects of the integration of blockchain and IPFS in smart urban environments and discuss their findings about enhancing data security and privacy and optimizing efficiency. The incorporation of IPFS with Blockchain to improve smart cities' data storage and retrieval systems has been explored in detail, showing a significant boost in data protection, scalability, and how the enormous data generated from IoT devices is managed [5]. Some authors have proposed a framework to increase IoT device security in smart cities based on blockchain with reference to data exchange and communications security in smart city environments [6]. A systematic literature review on using blockchain technology in smart cities mentions its application in environmental applications, energy applications, and secure communication and discusses how blockchain may solve various issues occurring in smart cities [7]. The implementation of consortium blockchain for secure transmission and archiving of data in VANET within smart cities has been considered, highlighting the advantages of providing secure and dependable data in a Changing environment [8]. Figure 1 portrays relevant publications by researchers in the past 3 years; in the very next section, Table 1 presents a comparative analysis of multiple studies related to blockchain in smart cities.

Figure 1: IPFS hash in Blocks

Table 1
A comparative analysis of previous studies on blockchain in Smart cities

Reference	Methodology	Technology Used	Outcome	Advantages	Limitations
[9]	Experimental	Blockchain, IPFS	Improved data storage and retrieval efficiency in smart cities	Enhanced data security and scalability	Initial setup complexity, integration issues
[10]	Theoretical	Blockchain, IoT	Enhanced IoT device security within smart cities	Secure data exchange, robust communications	Scalability issues with blockchain
[11]	Framework Design	Blockchain, Privacy Techniques	Addressed data poisoning and inference attacks in IoT networks	Ensures privacy and transparent processing	High computational overhead
[12]	Survey	Blockchain	Reviewed security challenges and solutions for IoT-based smart cities	Trustworthy data management	Energy consumption, lack of standardization
[13]	Case Study	Blockchain, IPFS	Blockchain-based power metering system for smart grids	Scalability, secure energy management	Implementation complexity

3. Smart contract

Smart contracts are self-contained software applications running on a blockchain; they resemble standard contracts but are written in proper programming languages such as Solidity. These contracts immediately execute the agreement's provisions written on a blockchain database. As shown in Figure 2 below, smart city nodes, denoted as 1 and 2,3,4, can record their transactions through a smart contract connected to the blockchain. Once this transaction joins a block, it cannot be altered anymore, which proves the effectiveness of the blockchain service[14].

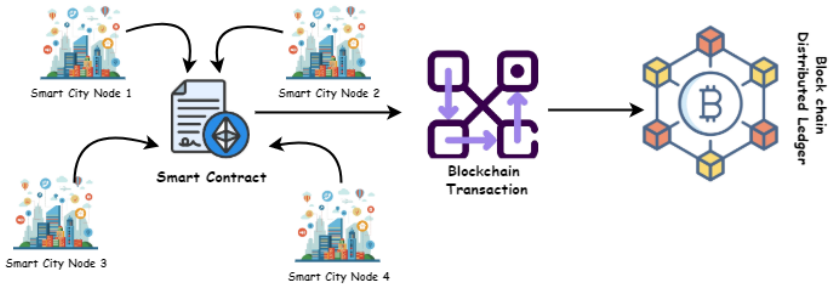

Figure 2: Smart contract Working in proposed case studies

3.1. Blockchain working with IPFS

This paper aims to discuss incorporating blockchain technology with the InterPlanetary File System. IPFS can efficiently address the significant amount of data produced in smart city settings[15]. Traditional blockchains, including Bitcoin, process transactions primarily as small hash values, which can be infeasible because the algorithms use a small amount of data compared to other methods. However, in the case of a smart city, the situation is rather different. Smart cities generate significant amounts of data from multiple sources like Internet of Things (IoT) devices, traffic controlling and monitoring systems, environment sensors, etc. Urban infrastructural elements continuous generation of data results in a marked rise in the costs borne by the consumers. Volume of data creates some issues when it comes to storing this information in a blockchain ledger [16].

It is also essential to understand how traditional blockchain storage works and what problems arise when the amount of data is huge, produced in a smart city. It is impracticable to store all this data directly on the blockchain, resulting in bloating and an extensive IT infrastructure to deal real-time transaction appropriately. To address all these challenges, this paper recommends utilizing IPFS, a distributed file system ideally designed for data storage and retrieval. In this way blockchain can only store smaller cryptographic hashes of the more significant data stored in the IPFS structures rather than the actual datasets[17]. This helps to make each block in the blockchain unique and also challenging to alter. It may include an IPFS hash that links to the specific dataset located in IPFS[18]. The following are the benefits that blockchain and IPFS bring to smart city applications: Firstly, by decoupling the data storage from the blockchain, the system can significantly optimize the amount of data that has to be stored on the blockchain. Reducing some of the drawbacks associated with scalability and frequency of transaction[19]. This is particularly important as the amount of data grows, this structure enables the blockchain to process a large number of transactions without clogging bottlenecks. Additionally, IPFS allows for quick access to different pieces of information, which is crucial for the immediate decision-making capabilities essential for smart cities. Also, this synergy improves the security and the reliability of the data collected. While IPFS provides a distributed manner of data storage, the blockchain ensures the originality and reliability of data.

It is also important to note that the data can be validated with the help of an immutable distributed ledger[20]. This combination enhances the dependability of the data utilized in smart city applications and stakeholders' trust. Decision-makers in the city council, government personnel in departments that deliver these services, to members of the public[21]. Further, the concept of deploying IPFS unveils the

application potential within smart cities as follows: Improved and integrated disaster response measures, traffic monitoring, and energy supplies Networks. Hence, this proposed integrated framework will pave the way for a more robust and responsive smart city by efficiently handling big data without impacting its processing capability. Hence, the integration of blockchain and IPFS is a sound solution for considering the problem of managing data in smart cities. This integration increases the capability of the structure of major cities to address the rising needs for data storage infrastructure. For that reason, smart cities can progress in a greater way in their attempts to implement dependable data processing and safety measures.

As depicted in Figure 2 below, each block shown could contain an IPFS hash pointing to any other data set stored in the IPFS. This integration helps the blockchain handle big data without compromising performance, which is desirable for the envisioned smart city system.

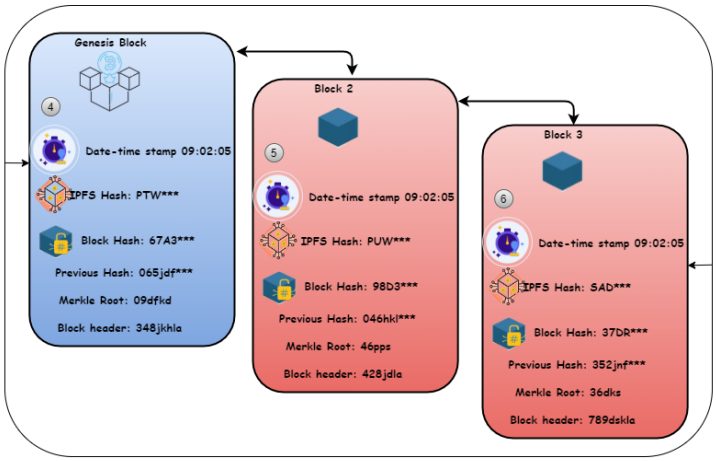

Figure 3: IPFS hashes in Blocks

4. Proposed Framework

Our proposed framework encompasses a smart city architecture and multiple data feed points and demonstrates stored and deployable datasets using blockchain through IPFS. To this end, each block in the blockchain can contain an extra key that consists of an IPFS hash. Several important benefits arise from the combination of blockchain and IPFS. As a file distributing storage protocol, the IPFS guarantees convenient and secure availability of the file for the user nodes[22]. It removes the need for duplicate data copies at different places since IPFS addresses data by hashes, guaranteeing data immutability and persistence on the network. This also facilitates faster access and use of data and cuts across the bandwidth by allowing users to exchange data through IPFS addressing[23] directly. Moreover, IPFS makes integrated and versioned data available with offline capabilities in its structure complemented by the Merkle DAG, which guarantees that the data is unambiguously identified, fixed, and can exist offline. Figure 4 below portrays our proposed framework.

4.1. Experimental setup and Validation

The following section explains our experimental setup and system validation.

4.1.1. Hardware Requirements

To perform the validation experiment of our proposed model, we require hardware with the following specifications, which includes the Intel 9th Generation i7 CPU, NVIDIA GTx 1650, 1024 GB PCIe SSD, and 32 GB of DDR4-2666 MHz RAM. These specifications offer reasonable guarantee that the system has enough computing power and graphics, storage, and memory to help with our experiment.

4.1.2. Software Environment

The following software environment is required: Ganache CLI for Local Ethereum blockchain creation and debugger and the Meta-Mask Ethereum Browser Extension for managing Ethereum accounts and transactions. Ideally, the system should run in Windows 10 for easy host synchronization and streamlined performance. Development will be conducted using the Solidity programming language. Node v8. for web applications, server-side JavaScript executions, and Web3. js as an interface for dealing with the Ethereum blockchain. Furthermore, the REMIX Integrated Development Environment will be used to script and compile smart contracts and their deployment.

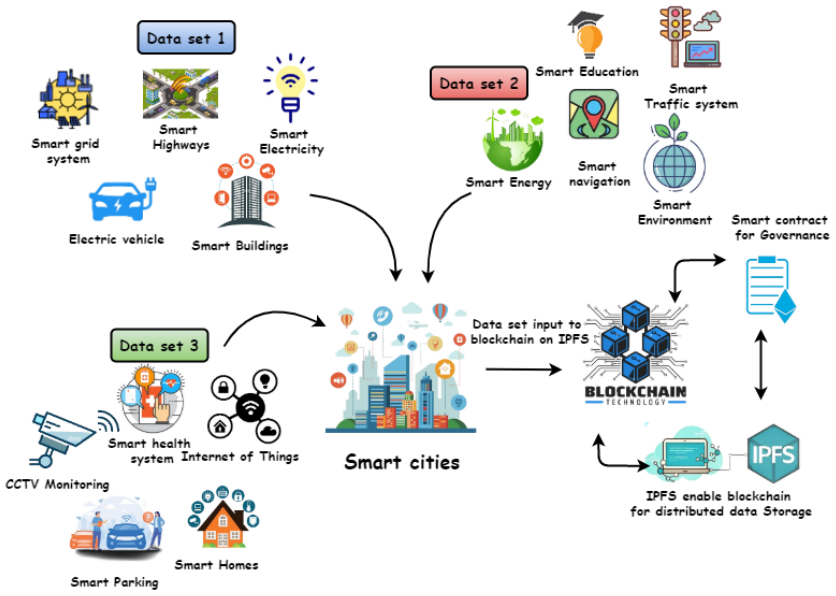

Figure 4: Our Proposed Framework

4.2. Environmental Disaster Scenario

To validate our proposed model, scenarios have been utilized to simulate a smart city ecosystem based on an Ethereum blockchain with data nodes. In one such scenario, an accident occurs on a highway, initially detected by sensors on the road. This detection promptly triggers the activation of specific smart contracts deployed on the blockchain, as presented in Figure 5. The The experiment also used the ganache-CLI-generated set of Private-Public keys as an assumed node role. Four smart contracts for simulation have been identified, each designed to fulfill specific functions within this system.

Below Figure 6 depicts all smart contracts for our given scenario which are coded in solidity and deployed successfully in Ethereum remix

- **InfoEnvAgency.sol:** This smart contract in Figure 7 identifies the disaster with the help of environmental sensors installed in the city. This kit automatically alerts the nearest environmental agency with the exact GPS coordinates.

- **InfoNearShelter.sol:** Ascertains the closest shelters or safe areas that affected people can temporarily evacuate to. Notifications are made to the residents and the authorities overseeing the shelters or centers Figure 8.

- **AllocateRescueRes.sol:** Dispatches the rescue equipment, such as boats, trucks, and personnel, to evacuate affected people to shelters. This contract in Figure 9 facilitates cooperation among various agencies responding to disaster cases.

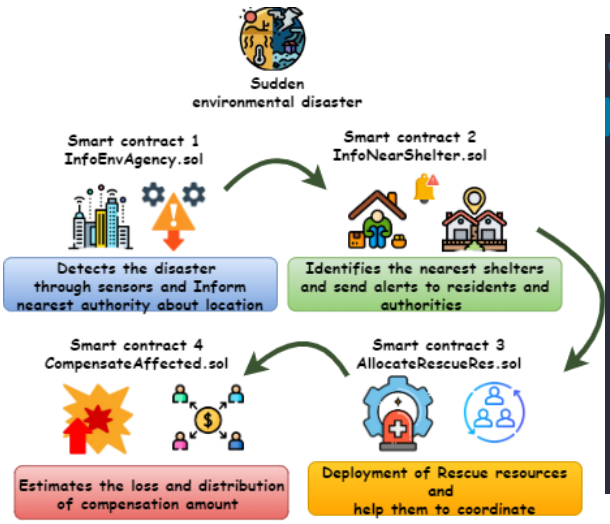

Figure 5: Framework Smart contracts.

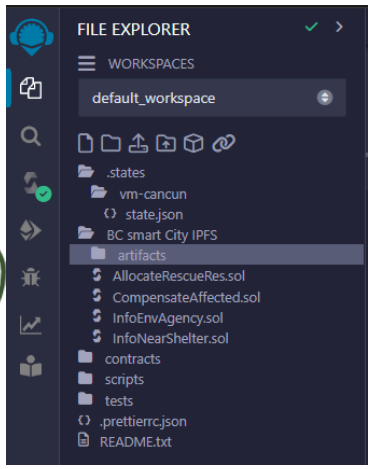

Figure 6: Smart contracts code deployed on Remix.

- **CompensateAffected.sol:** This contract in Figure 10 addresses the reimbursement for the damaged inhabitants or companies. Its usage of the distributed ledger allows for clear tracking of the fund distribution from customers and insurers.

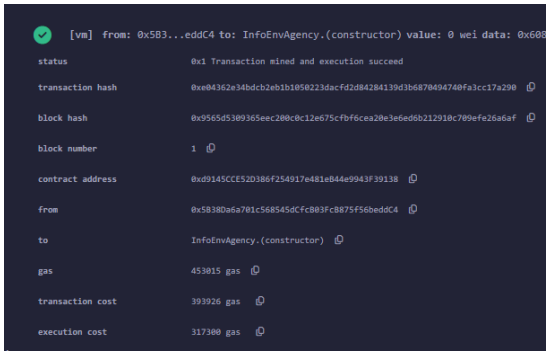

Figure 7: InfoEnvAgency smart contract.

Figure 8: InfoNearShelter smart contract.

Figure 9: AllocateRescueRes smart contract.

Figure 10: CompensateAffected smart contract.

The algorithms below present a quick information flow of smart contracts in proposed scenarios.

Algorithm 1 Disaster Detection and Alert System

```
function DETECT_AND_ALERT_DISASTER
    # Initialize sensor data collection
    start_sensor_data_collection()
    while true do
        sensor_data ← read_sensor_data()
        if is_abnormal(sensor_data) then
            break
        end if
    end while
    # Retrieve GPS coordinates
    GPS_coordinates ← get_GPS_coordinates()
    # Determine nearest environmental agency
    nearest_agency ← find_nearest_agency(GPS_coordinates)
    # Alert the nearest agency
    alert_agency(nearest_agency, GPS_coordinates)
end function
```

Algorithm 2 Evacuation and Shelter Notification

```
function ASCERTAIN_AND_NOTIFY_SHELTERS
    # Determine the nearest shelters or safe areas
    shelters ← find_nearest_shelters()
    for each shelter in shelters do
        # Notify affected residents
        notify_residents(shelter)
        # Notify authorities overseeing the shelter
        notify_authorities(shelter)
        # Log notification details for the shelter
        log_notification(shelter)
    end for
    # Ensure all notifications are confirmed
    confirm_notifications()
    # Provide confirmation or summary of notifications
    return "Notifications sent to residents and authorities"
end function
```

Algorithm 3 Dispatch Rescue Equipment

```
function DISPATCH_RESCUE_EQUIPMENT
    # Allocate rescue resources and coordinate disaster response
    rescue_equipments ← allocate_resources()
    for each equipment in rescue_equipments do
        # Dispatch equipment to evacuate affected people
        dispatch(equipment)
    end for
    # Facilitate cooperation among responding agencies
    cooperate_with_agencies()
    # Provide confirmation or summary of dispatch operations
    return "Rescue equipment dispatched and agencies coordinated"
end function
```

Algorithm 4 Compensate Affected Entities

```
function COMPENSATE_AFFECTED
    # Process reimbursement for damaged entities
    claims ← process_claims()
    for each claim in claims do
        # Verify and approve claims
        verify_and_approve(claim)
        # Distribute compensation from customers and insurers
        distribute_compensation(claim)
    end for
    # Track fund distribution using distributed ledger
    track_fund_distribution()
    # Provide confirmation or summary of the compensation process
    return "Claims processed, compensation distributed, and funds tracked"
end function
```

5. Results evaluation and discussion

The evaluation of our blockchain-based smart city framework demonstrates how it can be useful in practical scenarios for developing smart cities. Based on this study's findings, smart contracts' effectiveness

in disaster management was evident in the environmental disaster scenario. InfoEnvAgency.sol contract also allowed immediate disaster identification and reporting to the closest environmental agency with GPS coordinates. InfoNearShelter.sol contract effectively helped identify nearby shelters and provide timely evacuation of occupants. AllocateRescueRes.sol contract helped reduce the confusion involved in dispatching rescue resources and put all agencies on the same page. CompensateAffected.sol also handled the compensation process efficiently with the help of blockchain, which has a record of all forms of transactions. Screenshots of these smart contracts further demonstrate the successful deployment and execution of the contracts.

Furthermore, we have implemented two more real-life use case scenarios. Their results are presented in tables specified with data obtained, confirming the proposed model's effectiveness in real-life scenarios. From these tables, it is clear that within the provided scenarios, environmental, traffic, and energy, the proposed blockchain framework and IPFS handle data well.

In the traffic management scenario, the TrafficFlowOptimize. sol contract was dynamic in adjusting the traffic light timings depending on the current traffic conditions, thus improving traffic flow and public safety. Likewise, in the energy grid management scenario, load balancing. sol did manage power distribution to avoid overloads, RenewableEnergyBoost. sol supported the application of excess renewable generation and DemandResponse. sol promoted conservation particularly during high demand occasions. These results have underscored the capability of the proposed framework to achieve a range of urban objectives efficiently. Blockchain and IPFS with smart city applications promote efficiency in response, transparency, and usage of resources. The tables below present the experimented node details for multiple scenarios [24]. Table 2 presents node details in environmental disaster scenarios, Table 3 presents node details for Traffic management and public safety scenarios, and Table 4 presents details about energy grid management.

Table 2
Node Details in Environmental Disaster Scenario

Node Name	Node Type	Public Key	Initial Ethers	Final Ethers	Total Blocks Generated
Smart City	Env. Sensor 1	0x90F8bf6Ad	0	9	50
Smart City	Env. Sensor 2	0x22d491B0f43	0	5	60
Smart City	Env. Sensor 3	0xE11BA25E599	0	7	46.77
Smart City	Rescue Ops	0xd03ea8622350	0	12	70
Smart City	Shelter Mgmt	0x95cED1cd0	0	9	57.36

Table 3
Node Details for Traffic Management and Public Safety

Node Name	Node Type	Public Key	Initial Ethers	Final Ethers	Total Blocks Generated
Smart Highway	Smart City	0xFFcf8FD21k1	0	8	17.43
Smart Health	Smart City	0x22d491Bdb2	0	12	57.69
Monitoring	Smart City	0xE11BA2b4D91E	0	6	46.77
Data Centers	Smart City	0xd03ea86614	0	15	42.95
Smart Traffic	Smart City	0x95cED9ba40	0	10	57.36

Table 4
Node Details for Energy Grid Management

Node Name	Node Type	Public Key	Initial Ethers	Final Ethers	Total Blocks Generated
Load Balancing	Smart City	0x90F8bf6A4f32	0	20	85
Renewable Energy	Smart City	0xFFcf8FD72a	0	18	90
Demand Response	Smart City	0x22d491Bd303	0	15	70

6. Gas Cost comparison

Figure 11 in the gas cost comparison illustrates the differences in the transaction costs in various smart city scenarios. Based on this analysis, it is possible to understand how the specificity of smart contracts and blockchain operations affect the total cost, including advice on managing gas consumption.

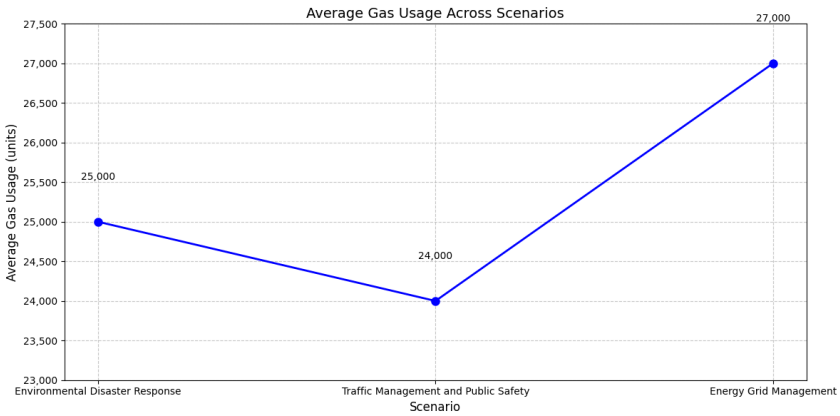

Figure 11: Gas Cost Comparison of Different Smart Contract Scenarios

7. Attributes Comparison with Recent Studies

Table 5 compares our proposed system with recent state-of-the-art papers across six attributes: Data Privacy, Real-Time Data Handling, Transparency and Accountability, Scalability, Data Reliability, and Interoperability. Our system outperforms the reviewed approaches in several key areas. Our approach excels in Data Privacy, effectively safeguarding sensitive information across all scenarios. Real-Time Data Handling is another strength, with our system managing and processing data promptly, unlike some other models. We maintain high standards of Transparency and Accountability, ensuring clear oversight, which is lacking in several reviewed papers.

8. Analysis of Our Findings

This paper reveals that combining blockchain and IPFS is crucial for improving smart city data management. Combining large-scale data storage systems like IPFS and the immutability of records through blockchain solves problems such as scalability and retrieval of data. From the tables indicated earlier in this paper, it is evident that deploying this integrated framework pays great dividends in various scenarios. Particularly in the case of environmental disasters, the framework facilitates accurate and

Table 5
Comparative Analysis of Our Model

Attributes	[13]	[14]	[15]	[16]	[17]	**Our Proposed System**
Data Privacy	×	×	×	✓	×	✓
Real-Time Data Handling	✓	✓	×	×	✓	✓
Transparency and Accountability	×	×	✓	✓	×	✓
Scalability	✓	✓	✓	×	✓	✓
Data Reliability	×	×	✓	✓	×	✓
Interoperability	✓	✓	×	✓	✓	✓

timely identification of disasters and subsequent alerting, coordinated evacuation, and organization of rescue missions. In traffic management, it fosters traffic flow and public measures that increase safety on the roads[17]. Furthermore, the system enables load, renewable energy, and demand response balances in energy grid management. These scenarios show how our framework is useful in practice because it optimizes response and data protection and achieves better efficiency in various smart city use cases.

8.1. Limitations and Future Research Directions

This study identifies several concerns that affect the practical usage of incorporating IPFS with Ethereum blockchain in smart cities. One limitation found in the simulation was that the architecture depicted needed to be bigger. However, this is due to necessary limitations, and effectively managing such large datasets presents challenges[20]. In terms of scalability, the application of blockchain technology poses challenges based on the real-time processing and storage of big data generated by high traffic, having high velocity, and evoking concerns of high variability and low credibility. Reliability, based on redundancy by methods such as Reed-Solomon codes, is an element of IPFS that remains to be solved. It is imperative to overcome these limitations for the progressive implementation and enhancement of smart cities utilizing blockchain technology[25].
Future research into integrating privacy and security in smart cities using blockchain and IPFS can explore several vital areas[26].First, we need more actual scenarios to measure the effectiveness of the introduced framework of various cities. This type of solution would focus heavily on scalability and where it would fit in the existing situation. City infrastructure [27]. One possible area of focus is enhancing the security of privacy in smart contracts with a special interest in protected use cases like health care and identity personal data. These mechanisms must, conform to regulations like the GDPR. Another worthwhile research is to design solutions that are more in the favor of customers. That allows citizens to own their data while adopting new smart city solutions [28]. Lastly, exploring the capability of promising technologies incorporated in AI and machine learning to bolster blockchain solutions in smart cities could generate innovative approaches to solving multifaceted urban management problems. security [29][30].

9. Conclusion

This paper proposes a solid architecture that enlists blockchain and IPFS to address security and privacy issues in smart city data management. Our framework was validated by developing three real-time controls: environmental disaster control, traffic control, and controls involved in energy transmission. The findings clearly show that Despite these improvements, data privacy has been found efficient, and real-time handling of schema and system efficiency have been found to improve IPFS in data storage. A

comparison of our system with previous research exhibits a higher efficiency of the proposed system in primary measures like transparency, scalability, and interoperability. However, the authors noted some limitations associated with big data analysis, such as scalability issues and challenges in processing big data sets affordably. The mentioned drawbacks should be addressed in subsequent studies to make a wider use of blockchain in smart cities. The advancement of this integrated framework will improve the general optimization of smart cities, security, sustainability, and the overall lifestyle of the citizen.

Acknowledgments:
This publication has emanated from research conducted with the financial support of Science Foundation Ireland under Grant number 23/PSF/12107.

References

[1] Y. Gao, A. Zhang, S. Wu, J. Chen, Blockchain-based multi-hop permission delegation scheme with controllable delegation depth for electronic health record sharing, High-Confidence Computing 2 (2022) 100084.

[2] L.-Y. Yeh, N.-X. Shen, R.-H. Hwang, Blockchain-based privacy-preserving and sustainable data query service over 5g-vanets, IEEE Transactions on Intelligent Transportation Systems 23 (2022) 15909–15921.

[3] L.-Y. Yeh, N.-X. Shen, R.-H. Hwang, Blockchain-based privacy-preserving and sustainable data query service over 5g-vanets, IEEE Transactions on Intelligent Transportation Systems 23 (2022) 15909–15921.

[4] M. I. Khalid, I. Ehsan, A. K. Al-Ani, J. Iqbal, S. Hussain, S. S. Ullah, et al., A comprehensive survey on blockchain-based decentralized storage networks, IEEE Access 11 (2023) 10995–11015.

[5] I. Ehsan, A. Mumtaz, M. I. Khalid, J. Iqbal, S. Hussain, S. S. Ullah, F. Umar, Internet of things-based fire alarm navigation system: A fire-rescue department perspective, Mobile Information Systems 2022 (2022) 3830372.

[6] P. Kumar, R. Kumar, G. Srivastava, G. P. Gupta, R. Tripathi, T. R. Gadekallu, N. N. Xiong, Ppsf: A privacy-preserving and secure framework using blockchain-based machine-learning for iot-driven smart cities, IEEE Transactions on Network Science and Engineering 8 (2021) 2326–2341.

[7] H. He, S. Bin, Y. Chen, Research on the blockchain digital capability platform for "no proof city", in: 2023 2nd International Conference on Artificial Intelligence and Computer Information Technology (AICIT), IEEE, 2023, pp. 1–4.

[8] L. Amasala, M. Ponnuru, P. Srideviponmalar, Secure goods storage and anti-theft approach using ethereum blockchain, Procedia Computer Science 233 (2024) 1–11.

[9] H. R. Hasan, A. Musamih, K. Salah, R. Jayaraman, M. Omar, J. Arshad, D. Boscovic, Smart agriculture assurance: Iot and blockchain for trusted sustainable produce, Computers and Electronics in Agriculture 224 (2024) 109184.

[10] A. Musamih, K. Salah, R. Jayaraman, I. Yaqoob, Y. Al-Hammadi, J. Antony, Blockchain-based solution for covid-19 vaccine waste reduction, Journal of Cleaner Production 372 (2022) 133619.

[11] D. Hanggoro, J. H. Windiatmaja, A. Muis, R. F. Sari, E. Pournaras, Energy-aware proof-of-authority: Blockchain consensus for clustered wireless sensor network, Blockchain: Research and Applications (2024) 100211.

[12] O. Popoola, M. Rodrigues, J. Marchang, A. Shenfield, A. Ikpehia, J. Popoola, A critical literature review of security and privacy in smart home healthcare schemes adopting iot & blockchain: problems, challenges and solutions, Blockchain: Research and Applications (2023) 100178.

[13] N. Mahmoud, A. Aly, H. Abdelkader, Enhancing blockchain-based ride-sharing services using ipfs, Intelligent Systems with Applications 16 (2022) 200135.

[14] N. A. Ugochukwu, S. Goyal, A. S. Rajawat, C. Verma, Z. Illés, Enhancing logistics with the internet of things: a secured and efficient distribution and storage model utilizing blockchain innovations and interplanetary file system, IEEE Access (2023).

[15] M. Abbasi, J. Prieto, A. Shahraki, J. M. Corchado, Industrial data monetization: A blockchain-based industrial iot data trading system, Internet of Things 24 (2023) 100959.

[16] V. Lukaj, F. Martella, M. Fazio, A. Galletta, A. Celesti, M. Villari, Gateway-based certification approach to include iot nodes in a trusted edge/cloud environment, in: 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), IEEE, 2023, pp. 237–241.

[17] F. Altamimi, W. Asif, M. Rajarajan, Dads: Decentralized (mobile) applications deployment system using blockchain: Secured decentralized applications store, in: 2020 International Conference on Computer, Information and Telecommunication Systems (CITS), IEEE, 2020, pp. 1–8.

[18] I. Ehsan, M. I. Khalid, M. Helfert, M. Ahmed, Chain links on wheels: A security scheme for iov connectivity through blockchain integration, Association for Computing Machinery, New York, NY, USA, 2024. URL: https://doi.org/10.1145/3664476.3670457. doi:10.1145/3664476.3670457.

[19] M. I. Khalid, M. Ahmed, J. Kim, Enhancing data protection in dynamic consent management systems: formalizing privacy and security definitions with differential privacy, decentralization, and zero-knowledge proofs, Sensors 23 (2023) 7604.

[20] M. I. Khalid, M. Ahmed, Blockchain based dynamic consent management systems for enhancing quality of life for people with disabilities, in: 2023 IEEE International Smart Cities Conference (ISC2), IEEE, 2023, pp. 01–07.

[21] Y.-J. Su, C.-H. Chen, T.-Y. Chen, C.-W. Yeah, Applying ethereum blockchain and ipfs to construct a multi-party used-car trading and management system, ICT Express 10 (2024) 306–311.

[22] M. Helfert, Gdpr-compliant data breach detection: Leveraging semantic web and blockchain, Good Practices and New Perspectives in Information Systems and Technologies: WorldCIST 2024, Volume 6 (????) 3.

[23] M. I. Khalid, M. Ahmed, K. Ansar, M. Helfert, Leveraging blockchain technologies for secure and efficient patient data management in disaster scenarios, in: World Conference on Information Systems and Technologies, Springer, 2024, pp. 12–21.

[24] M. I. Khalid, M. Ahmed, M. Helfert, J. Kim, Privacy-first paradigm for dynamic consent management systems: Empowering data subjects through decentralized data controllers and privacy-preserving techniques, Electronics 12 (2023) 4973.

[25] S. Liu, Q. Zheng, A study of a blockchain-based judicial evidence preservation scheme, Blockchain: Research and Applications (2024) 100192.

[26] H. Malik, T. Anees, M. Faheem, M. U. Chaudhry, A. Ali, M. N. Asghar, Blockchain and internet of things in smart cities and drug supply management: Open issues, opportunities, and future directions, Internet of things (2023) 100860.

[27] L.-Y. Yeh, N.-X. Shen, R.-H. Hwang, Blockchain-based privacy-preserving and sustainable data query service over 5g-vanets, IEEE Transactions on Intelligent Transportation Systems 23 (2022) 15909–15921.

[28] M. Son, H. Kim, Blockchain-based secure firmware management system in iot environment, in: 2019 21st International Conference on Advanced Communication Technology (ICACT), IEEE, 2019, pp. 142–146.

[29] Y. Liang, Y. Li, B.-S. Shin, Blockchain-based crowdsourcing for human intelligence tasks with dual fairness, Blockchain: Research and Applications (2024) 100213.

[30] I. Ehsan, M. Irfan Khalid, L. Ricci, J. Iqbal, A. Alabrah, S. Sajid Ullah, T. M. Alfakih, A conceptual model for blockchain-based agriculture food supply chain system, Scientific Programming 2022 (2022) 7358354.