

# Decentralized Traffic Management

Raghu P<sup>1</sup>, Jones Lejo J<sup>2</sup>, Kokila M B<sup>3</sup>, Kusumanjali S<sup>4</sup>, G Harshad<sup>5</sup>  
*Dept.of ISE, Cambridge Institute of Technology, Bangalore, India*

**Abstract**—Traffic congestion in urban areas leads to longer travel times, higher fuel consumption, and increased pollution. This project proposes a Decentralized Traffic Management System using blockchain-based Mobile Crowd Sensing (MCS) to address these issues. Participants use a mobile app to collect and share real-time traffic data, which is securely stored on a blockchain network, ensuring data authenticity, privacy, and decentralization. A trust-based algorithm selects reliable participants, while smart contracts manage automated rewards for contributors. The system improves traffic monitoring, enhances data security, and ensures fair compensation. Testing shows efficient performance with low latency. Future work will focus on scalability and real-world implementation.

**Index Terms**—Decentralized traffic management, blockchain, mobile crowd sensing (MCS), smart contracts, real-time traffic data, data security, trust-based recruitment, and urban mobility.

## I. INTRODUCTION

The development of network technologies, sensor devices, and connectivity has increased the deployment of Mobile Crowd Sensing (MCS), the next generation of the Internet of Things (IoT). MCS is a new knowledge base supported by smartphone sensors and incorporating human intelligence. MCS has become an application in cybersocial systems (CPSS) because it uses various approaches to provide solutions by combining knowledge from communication, computer science, computer networks, economics, psychology, and social sciences. Compared with traditional IoT systems, MCS has the advantages of wide visibility, strong spatiotemporal data understanding, strong deployment applicability, and simplicity. MCS has been widely used in different scenarios such as personalized healthcare, smart cities, environmental monitoring, and disaster recovery. It has also attracted the attention of education and business.

The topics studied in MCS include support mechanisms,

sensor data transmission, sensor performance, and sensor data extraction quality and service. Finally, this paper discusses blockchain-based MCS issues

[1] <https://ieeexplore.ieee.org/document/8949752> Smart factory is the representative of the reshaping of the information industry, smart industry-liefridai, the applicability and mobility of smart industrial systems. Data-driven business systems usually rely on data collected from statically deployed electronic devices. However, the spatial coverage of commercial sensor networks is limited due to the high installation and maintenance costs. In recent years, mobile crowd sensing (MCS) has emerged as a new sensing paradigm due to its advantages such as cost effectiveness, portability and scalability. However, due to their centralized design, MCS systems are always susceptible to malicious attacks and single factor failures. To do this, we integrate MCS with business systems without using any additional specialized tools. To address the shortcomings of traditional MCS systems, we propose a blockchain-based MCS system. Specifically, we use miners to analyze known data and generate the best reward (DRR) incentive to resolve the inconsistencies of various detection tasks. We also develop a data quality assessment tool to detect and reduce data bias. We implemented the BMCS model on Ethereum and conducted extensive testing in a real factory. Both tests and security assessments show that BMCS can protect businesses and increase system reliability.

[2] <https://ieeexplore.ieee.org/document/9126017> In this work, we create reward systems that can be used as a building block for crowdfunding apps. Our system allows users to send data and receive Bitcoin payments with privacy, and prevents service providers from linking data or payments back to users. We also

prevent bad user behavior, such as users trying to earn rewards by sending the same information multiple times. Most importantly, we ensure the integrity of the business; by relying on Blockchain, we eliminate the need for third-party trust in fair transactions. As a result, our system works very well because most of the underlying processes do not use the blockchain network. When they do, we only rely on simple Bitcoin transactions, not advanced transactions using smart contracts.[3]  
<https://ieeexplore.ieee.org/document/7913599>

In this paper, we propose UrbanCount, a fully distributed crowd counting protocol for densely populated cities. UrbanCount relies on mobile-to-device communication to make crowd estimates. Each node collects crowd estimates from other participants in the communication system and instantly integrates the estimates into its local estimate. The goal of UrbanCount is to analyze the local estimate to obtain global results while keeping the node private. We evaluate the proposed method through simulations of railway systems of mixed and realistic models. We also study the dependence between accuracy and density and show that in dense environments, the difference between local estimates does not exceed 2% for synthetic materials and 7% for real cases. In particular, we study the impact and loss of events, including studies on outages and communication technologies.

[4]<https://ieeexplore.ieee.org/document/7277045> In this paper, we proposed a mobile crowd sensing application based on Community Information Center Network to collect opportunistic sensing data in a limited area and limited radius strength. Compared with mobile group viewing applications, this application has better advantages. First, it supports data integrity with CICN features and uses simple communication models based on non-IP communication. Second, the data is collected using a name containing BLE beacon identifier. The application inherently supports user privacy and data integrity. We used multiple environmental sensors, Raspberry Pi, and BLE beacons at various locations in the building. The MCS application collects sensor data as users move around the smart home and maps the home sensors and environmental sensors. [5]  
<https://ieeexplore.ieee.org/document/7945390>

In this paper, we endorse effSense—an electricity-efficient and fee-powerful records importing framework, which makes use of adaptive uploading schemes within constant facts importing cycles. In each cycle, effSense empowers the participants with a dispensed choice making scheme to select the right timing and community to add facts. effSense reduces facts value for NDP users through maximally offloading facts to Bluetooth/WiFi gateways or DP users encountered; it reduces power intake for DP users with the aid of piggybacking statistics on a call or the usage of more strength-efficient networks instead of initiating new 3G connections. With the aid of leveraging the predictability of users' calls and mobility, effSense selects right importing techniques for both user types. Our evaluation with the MIT reality mining and Nodobo datasets indicates that effSense can reduce fifty five%–65% electricity intake for DP users, and 48%–52% statistics cost for NDP users, respectively, in comparison to conventional uploading schemes. Benefits: Key worries for DP and NDP users (strength consumption vs records value) are addressed simultaneously. Disadvantages: Negative overall performance. [6]<https://ieeexplore.ieee.org/document/7166062> In this paper, we take a look at a critical problem in MCS systems, specifically, incentivizing worker participation. We propose an incentive framework named Thanos that incorporates a critical metric called Quality of Information (QoI). We design fair and computationally efficient mechanisms for both single- and multi-minded combinatorial auction models, ensuring social welfare with a guaranteed approximation ratio. Benefits: Fair and computationally efficient mechanism with a focus on maximizing social welfare. Disadvantages: Complex methodology.[7]<https://ieeexplore.ieee.org/document/8345598> In this work, we propose using blockchain technology and smart contracts to orchestrate interactions between mobile crowdsensing providers and mobile users for spatial crowdsensing, where mobile users need to be at specific locations to perform tasks. Smart contracts act as automated processes on the blockchain to maintain user privacy and handle payments. We design a trustworthy, cost-optimal auction to minimize payments from crowdsensing providers to mobile users. Experimental results show that our privacy-preserving auction outperforms

existing approaches by ten times in cost efficiency for large numbers of mobile users and tasks. Benefits:

Trustworthy, cost-optimal auction mechanism. Disadvantages: Low performance and highly unreliable.

[8]<https://ieeexplore.ieee.org/document/8359258> introduces the first private and nameless decentralized crowdsourcing machine, ZebraLancer1, addressing key challenges of decentralizing crowdsourcing, including data leakage and identity breaches. The proposed outsource-then-show methodology effectively balances blockchain transparency with data confidentiality, a critical aspect for crowdsourcing use-cases. ZebraLancer ensures (i) a requester will not pay more than what the information deserves, as per the policy announced when the task is posted through the blockchain; (ii) every worker receives a payment based on the policy upon submitting data to the blockchain; (iii) these guarantees are achieved without a central arbiter and without exposing the data to the open blockchain. The transparency of the blockchain allows inferring personal data about employees and requesters through their participation history. However, anonymity could enable malicious workers to submit multiple times for rewards. ZebraLancer addresses this by allowing anonymous requests/submissions while maintaining accountability. It introduces a subtle linkability: if a worker submits twice to a task, submissions can be linked; otherwise, the worker remains anonymous and unlinkable across tasks. To achieve this, a unique cryptographic concept called common-prefix-linkable anonymous authentication is proposed. The authors observe that this novel authentication scheme may have independent significance. The protocol was implemented for a common image annotation task and tested on the Ethereum network, demonstrating the applicability of the protocol on the existing real-world blockchain. Benefits: The paper presents a general blockchain-based protocol enabling the first private and anonymous decentralized data crowdsourcing machine. Risks: Personal information may still leak.[9]

<https://ieeexplore.ieee.org/document/8455990>

proposes a decentralized crowdsensing structure leveraging blockchain technology to enhance attack resistance. Additionally, a hybrid incentive mechanism is introduced, integrating data quality, reputation, and financial factors to encourage participants to contribute their sensing data while deterring malicious behaviors. The proposed incentive model's effectiveness is validated through a blend of mechanism design concepts. Performance analysis and simulation results demonstrate that the hybrid incentive model is a reliable and efficient approach to promoting data security and incentivizing positive behavior in crowdsensing applications. Benefits: The performance evaluation and simulation results indicate that the proposed hybrid incentive model is a reliable and efficient means to promote data safety and encourage positive behavior in the crowdsensing utility. Disadvantages: The system does not focus on developing a more adaptive hybrid incentive model to address new challenges arising from dynamic changes in the demand for crowdsensing tasks.

## II. METHODOLOGY

1.device Initialization -undertaking initiators and individuals check in for the MCS utility.They put up their identities, public/non-public keys, and certificate to the closest miner.Miners verify identities using a consensus mechanism earlier than confirming participation.once verified, the assignment initiator submits the sensing assignment to the miners.The project is broadcasted to all registered members.2.Incentive Mechanism Deployed smart contracts control the role project and reward distribution."participant Profile agreement" and "Sensing task contract" determine payments primarily based on statistics excellent and participation.3.Sensory information uploading participants entire assigned obligations and upload sensory facts thru the miner.instantaneous-pay to the individuals obtain rewards immediately from the blockchain account.

4.Blockchain Integration Miners system evidence of labor (PoW) and create new blocks containing transaction records.Blocks are validated and brought to the blockchain.

clever contracts make sure automated, comfy transactions.

5.consider-primarily based Recruitment algorithm. A consider assessment model assesses participant reliability.trust ratings are primarily based on past accuracy, experience, and reputation.The system recruits participants with the highest trust values.

6.checking out & Validationone of a kind trying out techniques, which I nclude unit testing, integration trying out, and gadget testing, ensure overall performance and security.

#### ALGORITHM 1:

##### TRUST-BASED RECRUITMENT ALGORITHM:

```

1 Initialization TRUST[ ][ ], EXP[ ][ ], REP[ ] ;
2 out = 0;
3 foreach request R( i ) from user U( i ) do
4     foreach sensing task STR(i)( j ) do
5         Recruit( Pij users with highest
TRUST[Pij users ][
        U( i ) ] );
6         QoD( Sensing data from Pij users );
7         Update( EXP[U(i)][Pij users] );
8         Update( REP[ ] );
9         Update( TRUST[ ][ ] );
10    end
11    out ←out + QoS(R(i));
12 end
13 Return out

```

The algorithm aims to manage trust, experience, and reputation within a system that handles user requests involving sensing tasks. It begins by initializing three matrices: TRUST, which maintains trust levels between users; EXP, which tracks user experiences with specific sensing tasks; and REP, which stores the reputation scores of users. The variable out is initialized to 0 to accumulate the overall Quality of Service (QoS). As the algorithm processes each request R(i) from a user U(i), it iterates through all associated sensing tasks STR(i)(j). For each sensing task, the algorithm recruits P<sub>ij</sub> users with the highest trust scores relevant to the task. It then evaluates the Quality of Data (QoD) from the sensing data provided by these recruited users. Subsequently, it updates the EXP matrix to reflect the interaction between the requesting user U(i) and the recruited P<sub>ij</sub> users, the REP matrix to adjust reputation scores, and the TRUST matrix to incorporate changes due to new

experiences and updated reputations. After completing all sensing tasks for a request, the algorithm adds the QoS of the processed request to the out variable. Once all requests are processed, the algorithm returns the total out, representing the aggregated QoS. This approach ensures dynamic and adaptive management of trust, experience, and reputation, contributing to a high-quality service outcome.

#### ALGORITHM 2:

##### REPUTATION-BASED TRUST EVALUATION ALGORITHM

```

If acc ≥ 80
    Pos_rep++
Else
    Neg_rep++
Experience Count :
    When user post any information :
        Exp++
Check last updated date :
    If day_diff > 7
        Exp--
For all acc find avg accuracy
    Total_acc = ∑ acc
    Total_count ++
Trust count :
Trust_count = Total_acc / Total_count

```

The algorithm focuses on updating positive and negative reputation, experience, and trust based on user accuracy and activity. When the accuracy (acc) is 80 or above, the algorithm increases the positive reputation (Pos\_rep++); otherwise, it increments the negative reputation (Neg\_rep++). The experience count (Exp) is updated each time a user posts information by increasing the experience (Exp++). The algorithm also monitors the last updated date, and if the difference between the current day and the last update (day\_diff) exceeds 7 days, the experience is

decreased (Exp--). To calculate the average accuracy, the algorithm sums up all accuracy values ( $\text{Total\_acc} = \sum \text{acc}$ ) and increments the total count ( $\text{Total\_count}++$ ). Finally, the trust count ( $\text{Trust\_count}$ ) is calculated by dividing the total accuracy by the total count ( $\text{Trust\_count} = \text{Total\_acc} / \text{Total\_count}$ ), ensuring an accurate and fair representation of a user's trustworthiness within the system. This approach helps maintain a balanced evaluation by considering both the frequency of contributions and their quality. By continuously updating these metrics, the system promotes active and reliable user participation, enhancing overall service quality.

### III. PROPOSED METHODOLOGY

High-stage layout (HLD) excessive-degree layout represents the overall device layout, protecting device structure and database design. It establishes relationships among diverse modules and functions of the machine, together with information go with the flow, flowcharts, and facts structures. HLD gives an summary view of device capability and database structure, ensuring a complete information for developers, testers, and stakeholders. It consists of undertaking requirements, practical layout files, and database layout documentation. HLD serves as an vital element in multi-undertaking improvement, making sure compatibility between supporting components and aligning them with the system's typical objectives. the best-stage solution layout in brief outlines all structured structures, structures, merchandise, services, and methods while figuring out vital adjustments. furthermore, HLD incorporates concerns regarding industrial, criminal, environmental, security, protection, and technical dangers, problems, and assumptions. This ensures effective collaboration across groups and affords clarity on possession for targeted design sports. Contributions from numerous professionals across unique professional disciplines are required, emphasizing stop-consumer experience and system usability.

#### System Architecture

The diagram illustrates a Mobile Crowd-Sensing (MCS) Centralized Platform for Traffic Information. The platform involves five main components: Service Requester, Participants (Mobile Users), MCS Management, Crowd Data Processing, and Data

Collection Infrastructure. The process starts with the Service Requester sending a service request (Step 1) to the Applications and Services module. Participants, including Mobile Users, are recruited and assigned tasks (Step 2) through the Data Collection Infrastructure. Mobile Users then provide sensing data (Step 3), which is incentivized (Step 5) to encourage participation. The collected data is processed in the Crowd Data Processing module. MCS Management oversees security, privacy, incentive schemes, task creation, execution, and user recruitment. Finally, the processed information is sent as a service response (Step 4) back to the Service Requester, completing the information flow.

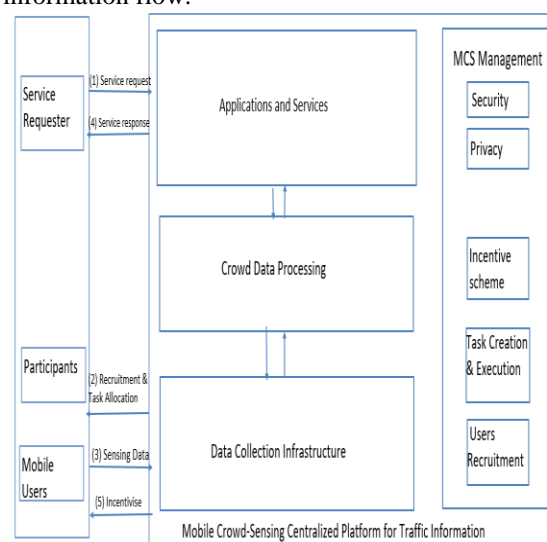


Fig1: System Architecture

#### Data Flow Diagram (DFD)

A Data Flow Diagram (DFD) is a graphical representation of how data flows within a system. It provides insights into data input, processing, and output. DFD models utilize a limited number of standardized symbols to represent system functions and the movement of data among them. The popularity of DFDs stems from their simplicity and ease of comprehension, making them an effective tool for visualizing hierarchical system structures.

DFDs depict high-level functions initially, followed by detailed sub-functions at lower levels, offering a progressive breakdown of system operations. The ability to present complex systems in a hierarchical manner enhances their accessibility and usability. DFDs serve as an essential tool in software

engineering for analyzing system processes and data interactions.

DFD components

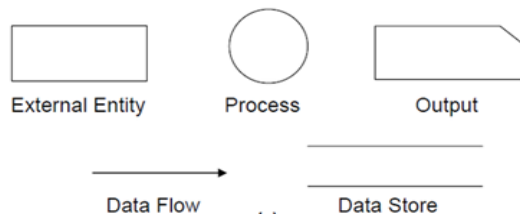


Fig 2 : DFD Components

Entities: Represent sources and destinations of data, depicted as rectangles.

Processes: Actions performed on data, represented as circles or rounded rectangles.

Data Storage: Represented as open-sided rectangles, indicating data retention locations.

Data Flow: Indicated by arrows, showing the movement of data from source to destination.

DFD :

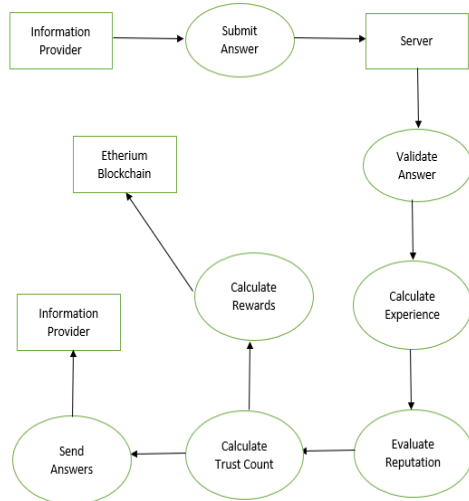


Fig 3: Data Flow Diagram

Use Case Diagram

A Use Case Diagram is a behavioral model representing system functionalities concerning users (actors), their goals (use cases), and interactions. This diagram illustrates the system's functional scope and external relationships. Use cases define the expected behavior of the system from an end-user perspective, ensuring a user-centric approach to system design. Query Sensing Reward Flow refers to the process in a Mobile Crowd-Sensing (MCS) system where users collect and submit sensing data in response to specific queries or tasks. The system verifies the data, processes it, and then provides rewards (such as

monetary incentives, points, or benefits) to users based on their contributions. This flow ensures user participation, data reliability, and efficient task completion.

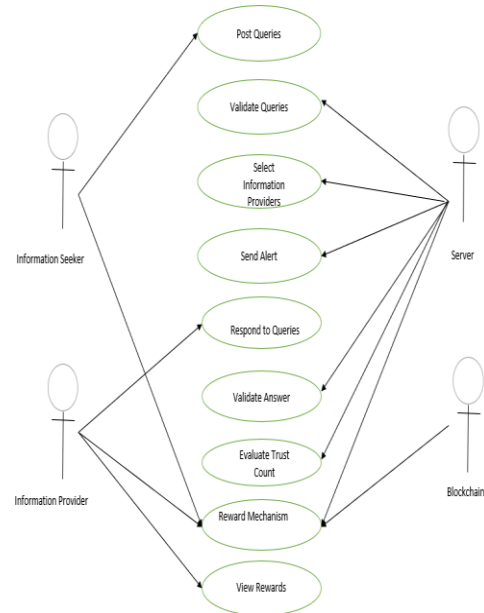


Fig 4: Crowd Sensing Query and Reward Flow

Key components of a Use Case Diagram include:

Actors: External entities interacting with the system.

Use Cases: Specific functionalities provided by the system.

System Boundary: Encapsulates system processes.

Sequence Diagram

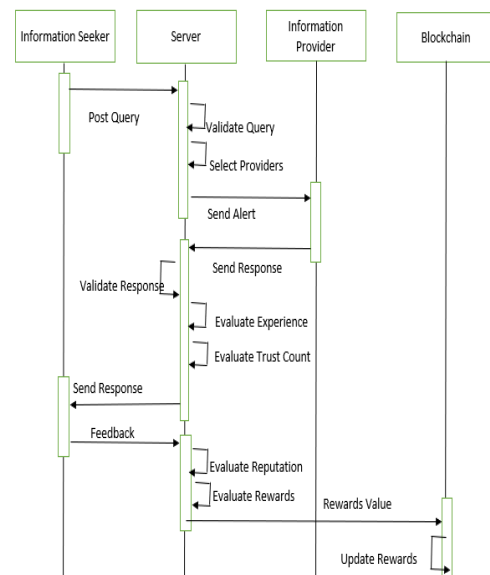


Fig 5: Blockchain-Based Query and Reward Sequence

### Activity Diagram

An Activity Diagram provides a flowchart-like visualization of system processes, detailing various operational sequences and decision points. It is used to model workflows, system behaviors, and functional interactions.

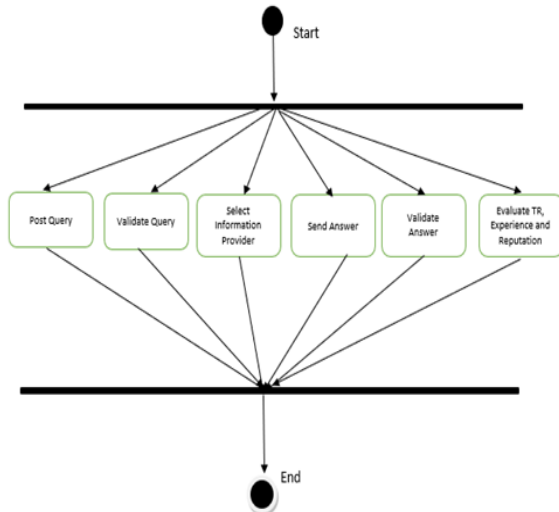


Fig 6: Decentralized Query Handling Workflow

## V. RESULTS AND DISCUSSION

### Sign up Page:

The screenshot shows the 'Registration Page' of the 'Trust\_Evaluation\_App'. It includes input fields for 'Name' (shravya), 'Email' (shravya@gmail.com), 'Phone Number' (8800880088), 'Gender' (Male, Female), and 'Profession'. A 'SUBMIT' button is at the bottom.

Fig 7: User Sign-up

The User Sign-Up process allows new users to register for the decentralized traffic management system. It typically includes entering details like name, email,

and password, ensuring secure authentication and access to traffic-related services.

### Home Page:

The screenshot shows the 'Home Page' of the 'Trust\_Evaluation\_App'. It features a 'Welcome' message and a list of options: 'UPDATE LOCATION', 'SELECT SERVICE', 'REMOVE SERVICE', 'UPDATE DATA', 'ASK FOR HELP', and 'CHECK REPUTATION'.

Fig 8: Home Page

The home page serves as the main dashboard of the decentralized traffic management system. It provides users with real-time traffic updates, navigation options, and access to key features like route optimization and traffic alerts.

### Update Location:

The screenshot shows the 'Update Location' page of the 'Trust\_Evaluation\_App'. It includes a 'Select' dropdown menu with options: 'Traffic', 'Transport', 'Healthcare', and 'Job'. A 'CHECK REPUTATION' button is at the bottom.

Fig 9: Update Location

The update location feature allows users to share their real-time location within the decentralized traffic management system.

### Update Data:

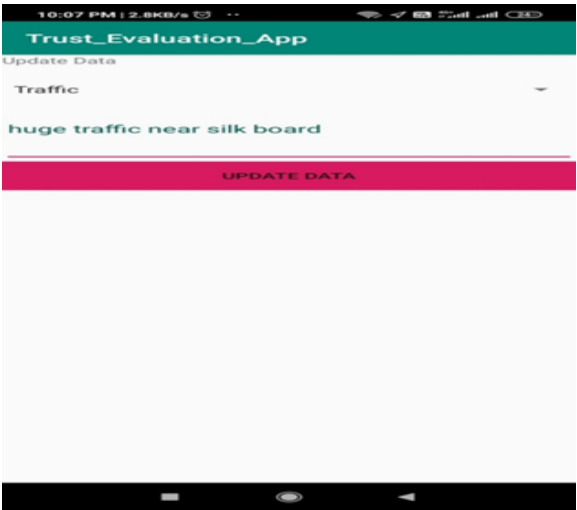


Fig 10: Update Data

The update data feature enables users to modify or upload traffic-related information within the decentralized traffic management system.

Statistics:

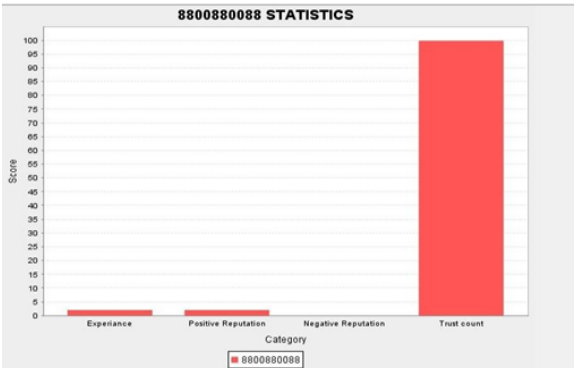


Fig 11

Trust Count: 99.817585, Pos reputation:2, Neg reputation:0

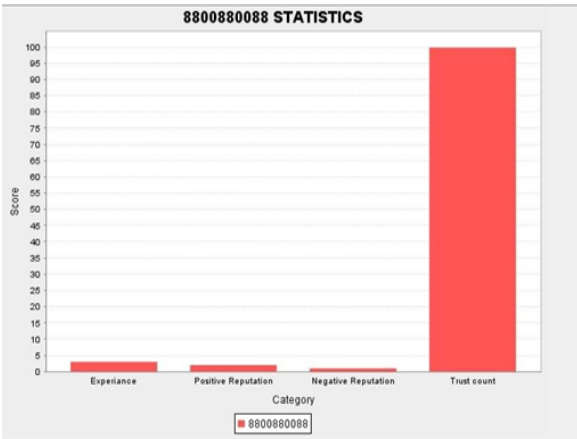


Fig 12

Trust Count: 99.817585, Pos reputation:2 ,Neg reputation:1

Check Reputation:

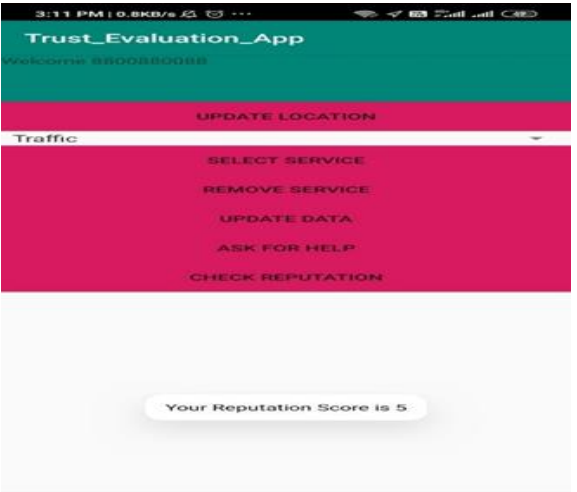


Fig 13: Reputation check

The check reputation feature allows users to view their trust score within the decentralized traffic management system. It is based on user contributions, data accuracy, and adherence to system guidelines, helping maintain reliability and accountability.

Existing Model	Proposed Model
Centralized system with a single point of control	Decentralized using blockchain for better distribution
Less secure, prone to data tampering	High security with blockchain verification
Low performance due to central processing	Faster processing with distributed nodes
Data can be manipulated or lost	Immutable and transparent data storage
Manual reward system, prone to unfairness	Automated smart contract-based incentives
Limited scalability due to central control	Highly scalable with decentralized architecture

VI. CONCLUSION

The work presented in this article has two main contributions toward solving the challenges of traffic.



First, it proposes a blockchain-based MCS framework with a novel set of smart contracts. Furthermore, the proposed system preserves the fairness of the sensory data market in cooperation with a secure reward allocation scheme aided by blockchain technology. It can also maintain the required market share for instant-pay participants while achieving sustainable sensory data provision. Finally, this article also discusses the future challenges in the cooperation of blockchain technology and MCS to enlighten future works. Consensus mechanisms, such as the computationally intensive PoW ensures data reliability. Therefore, in the future work, we will study the consensus mechanism of the blockchain to support improved efficiency and scalability.

#### REFERENCES

- [1] Y. Wang, Y. Yin, and Y. Li, "AI-based traffic flow prediction and smart city optimization," *J. Big Data Anal.*, vol. 9, no. 2, pp. 211–225, 2022.
- [2] S. Ghosh and P. Varakantham, "AI-driven optimization for smart urban traffic signal control," *Artif. Intell. Rev.*, vol. 55, pp. 1789–1812, 2021.
- [3] Z. Tang, H. Liu, and J. Luo, "Reinforcement learning in urban traffic signal control: A review," *IEEE Trans. Intell. Veh.*, vol. 6, no. 4, pp. 733–750, 2021.
- [4] L. Xie, X. Liu, W. Sun, and H. Liu, "A survey on blockchain technology for secure Internet of Things," *Future Gener. Comput. Syst.*, vol. 105, pp. 841–853, 2020. DOI: 10.1016/j.future.2019.12.002 ISSN: 0167-739X.
- [5] J. Shao, J. Liu, and Y. Zhang, "AI-empowered urban traffic prediction and management: A comprehensive review," *IEEE Access*, vol. 8, pp. 134763–134781, 2020.
- [6] X. Li, T. Li, Y. Wu, and Q. Liu, "Blockchain-based incentive mechanism for crowdsensing networks," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4148–4161, 2020.
- [7] F. De Souza, F. Duarte-Figueiredo, and F. Ferraz, "Intelligent traffic management systems using deep reinforcement learning," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 5, pp. 1875–1886, 2019.
- [8] J. Xie, J. Liu, X. Liang, and X. Shen, "Blockchain-based secure and trustworthy electronic medical records sharing scheme," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 2, pp. 462–475, 2019.
- [9] J. Hu, K. Yang, L. Hu, and K. Wang, "Reward-aided sensing task execution in mobile crowdsensing enabled by energy harvesting," *IEEE Access*, vol. 6, pp. 37604–37614, 2018.
- [10] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, 2018.
- [11] J. Liu et al., "Characterizing data deliverability of greedy routing in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 17, no. 3, pp. 543–559, Mar. 2018.
- [12] C. Zhao, S. Yang, P. Yan, Q. Yang, X. Yang, and J. McCann, "Data quality guarantee for credible caching device selection in mobile crowdsensing systems," *IEEE Wireless Commun.*, vol. 25, no. 3, pp. 58–64, Jun. 2018.
- [13] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Serv.*, vol. 14, no. 3, pp. 352–375, 2018.
- [14] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, 2017.
- [15] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Percom Workshops*, vol. 6, pp. 618–623, 2017.
- [16] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities: The Internet of Things is the backbone," *IEEE Consum. Electron. Mag.*, vol. 5, no. 3, pp. 60–70, 2016.
- [17] K. Christidis and M. Devetsikiotis, "Blockchain and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
- [18] R. Pryss, M. Reichert, J. Herrmann, B. Langguth, and W. Schlee, "Mobile crowd sensing in clinical and psychological trials—A case study," in *Proc. IEEE 28th Int. Symp. Comput.-Based Med. Syst.*, Jun. 2015, pp. 23–24.

- [19] L. G. Jaimes, I. J. Vergara-Laurens, and A. Raij, "A survey of incentive techniques for mobile crowd sensing," *IEEE Internet Things J.*, vol. 2, no. 5, pp. 370–380, Oct. 2015.
- [20] Y. Tobe, I. Usami, Y. Kobana, J. Takahashi, G. Lopez, and N. Thepvilojanapong, "VCity map: Crowdsensing towards visible cities," in *Proc. SENSORS*, Nov. 2014, pp. 17–20.
- [21] Z. Song, C. H. Liu, J. Wu, J. Ma, and W. Wang, "QoI-aware multitask-oriented dynamic participant selection with budget constraints," *IEEE Trans. Veh. Technol.*, vol. 63, no. 9, pp. 4618–4632, Nov. 2014.
- [22] N. Vastardis and K. Yang, "Mobile social networks: Architectures, social properties, and key research challenges," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1355–1371, 3rd, Quart. 2013.
- [23] P. Zhou, Y. Zheng, and M. Li, "How long to wait? Predicting bus arrival time with mobile phone based participatory sensing," in *Proc. 10th Int. Conf. Mobile Syst. Appl. Services*, 2012, pp. 379–392.
- [24] F. Calabrese, M. Colonna, P. Lovisolo, D. Parata, and C. Ratti, "Realtime urban monitoring using cell phones: A case study in Rome," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 1, pp. 141–151, Mar. 2011.
- [25] K. Yang, S. Ou, and H.-H. Chen, "On effective offloading services for resource-constrained mobile devices running heavier mobile Internet applications," *IEEE Commun. Mag.*, vol. 46, no. 1, pp. 56–63, Jan. 2008.
- [26] C. Fishwick, "Tomnod—the online search party looking for Malaysian Airlines flight MH370," *Guardian*, vol. 14, p. 37, Mar. 2014.