IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, April 2026
Impact Factor: 8.2

# HomoBlock-QC: A Homomorphic Encryption Assisted Blockchain Framework for Secure Crowdsensing Validation

**J. Siddharth[1], B. Balaji[2], S. Manoj Kumar[3], Jonnadula Narasimharao[4]**
UG Scholars, Department of Computer Science & Engineering[1-3]
Associate Professor, Department of Computer Science & Engineering[4]
CMR Technical Campus, Hyderabad, India

**Abstract:** *These days, more smart devices are built into everyday gadgets. One fresh way to gather information is called mobile crowd-sensing. People can now share what they see using personal devices. Still, most current setups rely on outside platforms run by others. Trusting those central sources completely remains uncertain. On top of that, safety and privacy matters often get brushed aside. When MCS runs, different user details plus their trust levels come into view, often out in the open - yet calculations tied to keeping those details private can't be checked. Here, we slot in blockchain within the MCS setup to create a system where data stays guarded, untouched, or falsely claimed, making sure payouts flow without bias. A fresh approach to picking participants includes privacy protections, letting everyone check outcomes - no outside judge needed. Because current crowd-sensing data raises privacy concerns along with efficiency issues during truth finding, an updated idea emerges: a private crowdsensing setup using repeated reasoning through secure shared calculations. The new round of tests shows that the updated method not only works but does so better than before. It means that users' personal information is that bit better protected while at the same time enabling reliable performance.*

**Keywords:** Mobile Crowd Sensing, Privacy Preservation, Quality Control, Blockchain Technology, Homomorphic Encryption, Secure Multiparty Computation, Data Integrity, Decentralized Validation, Smart Contracts

## I. INTRODUCTION

With the proliferation of powerful sensor embedded smartphones, crowdsensing has become a leading paradigm which leverages the pervasive smartphone users to collect data efficiently. In a typical crowdsensing application, a server posts the required sensing information and recruits a set of smartphone users to collect sensing data. After smartphone users send sensing data to the server, the server aggregates the sensing data to measure phenomena of common interest, i.e., real-time traffic conditions, environmental pollution quality or environmental noise pollution.

The accuracy of estimating the common interest depends on the high-quality contributions of highly skilled users. While providing the high-quality contributions, smartphone users consume their energy and the resources of their smartphones such as battery, storage and computing power. In addition, users may expose themselves to potential privacy threats as the sensed data contain time or location tags. Thus, the contributors should be given enough rewards to compensate for their resource consumption or potential privacy leaks.

As is known to all, a user wants to maximize her own profit, and may lie or impersonate others to get more payment. Therefore, the design of a secure and truthful incentive mechanism is particularly important. Many incentive mechanisms have been proposed and implemented, such as the reputation systems and monetary approaches. Reputation systems can help identify uncooperative users, but ignore a formal specification and analysis of the incentive types and suffer sybil attacks and whitewash attacks. Monetary approaches could be the most promising due

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, April 2026 Impact Factor: 8.2

to their explicit and flexible incentive methods. Most monetary schemes use pricing strategies to design truthful incentive mechanisms, in which the server and smartphone users cannot increase their utility by cheating or colluding with others.

Blockchain cryptocurrencies are provably decentralized secure, and have gained a noticeable popularity. The security of blockchain cryptocurrencies depends on a majority of the computing power instead of a central authority, thus eliminating the risks of one taking control over the system, generating inflation, or completely shutting down the system.

In this paper, we exploit a blockchain cryptocurrency to incentivize high skilled users to provide valuable or effective data for crowdsensing applications. We consider the scenario where there is one server, multiple smartphone users, and some miners in the blockchain system. When the server publishes a sensing task contained explicit evaluation criteria of sensing data quality in blockchain, it would make a certain deposit for promising to reward. The users who try to get the reward upload the sensing data to the peer-to-peer network. Instead of the server, the initiative miners are responsible for quantifying and validating the quality.

Our main contributions are listed as follows:

We propose a blockchain based secure crowdsensing incentive mechanism in which the miners' verifiable data quality evaluation can eliminate the security and privacy issues caused by a central authority.

We use an extended transaction syntax to implement a secure reward distribution in accordance with the predefined transfer conditions in the transaction script.

We propose a node cooperation privacy protection method for participating users to achieve k-anonymity privacy protection.

We further employ a theoretical analysis and simulation study to demonstrate the security and efficiency of our incentive mechanism.

## II. LITERATURE SURVEY

### A. Blockchain Security and Performance

Gervais et al. [2] introduced a novel quantitative framework to analyze the security and performance implications of various consensus and network parameters of Proof of Work (PoW) blockchains. Their framework allows capturing existing PoW-based deployments as well as PoW blockchain variants instantiated with different parameters, and objectively compare the trade offs between their performance and security provisions.

### B. Quality-Based Incentive Mechanisms

Peng et al. [4] proposed a quality-based incentive mechanism for crowdsensing, suggesting to "pay as how well you do." While continuous low quality sensing data could do harm to the availability and preciseness of crowdsensing based services, few existing incentive mechanisms have addressed the issue of sensing data's quality. Their mechanism estimates the quality of sensing data and offers each participant a reward based on her effective contribution.

### C. Social Trust Assisted Reciprocity

Gong et al. [5] exploited social trust assisted reciprocity (STAR) toward utility-optimal socially-aware crowdsensing. Mobile crowdsensing takes advantage of pervasive mobile devices to collect and process data for a variety of applications. They advocated a socially-aware crowdsensing system in which a cloud-based platform incentivizes mobile users to participate in sensing tasks by leveraging social trust among users.

### D. Reputation-Based Incentive Protocols

Zhang and van der Schaar [9] proposed reputation-based incentive protocols in crowdsourcing applications. Crowdsourcing websites emerged that allow requesters from all around the world to post tasks and seek help from an equally global pool of workers. However, intrinsic incentive problems reside in crowdsourcing applications as workers and requesters are selfish and aim to strategically maximize their own benefit. They proposed to provide incentives for workers to exert effort using a novel game-theoretic model based on repeated games, integrating reputation mechanisms into the existing pricing schemes.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, April 2026
Impact Factor: 8.2

## III. PROPOSED METHODOLOGY

### A. Proposed System

To overcome the above-mentioned issues, we employ Privacy Preserving Quality Control (PPQC) parameters on both servers and mobile users. The third-party server is replaced with Blockchain distributed servers which have inbuilt support for data integrity and tamper-proof storage. Data once stored cannot be altered and can only be accessed or viewed by authenticated users, ensuring privacy for mobile sensing users.

Mobile users who try to cheat the server are verified by employing a multiparty secure communication algorithm called Homomorphic encryption. This encryption allows users to directly perform mathematical operations without performing decryption. Mobile users encrypt sensed data and private information using the Multiparty Homomorphic algorithm and send it to the Blockchain server. The Blockchain server verifies the current user location with the existing location; the difference between current and existing location is considered as noise value. If there is a small difference in noise value, the Blockchain understands the user is sending truthful data. If noise has a large difference, the Blockchain considers this noise value as an attack and untruthful data.

### B. Modules Information

To implement this project, we have designed the following modules:

Generate Mobile Crowd Sourcing Network: Using this module, we generate random mobile sensing users which report data to the Publisher.

Submit Data: Using this module, we can select a desired mobile user which will report data to the server by applying privacy. The server then verifies the user's data by calculating noise value. If noise is smaller, a reward will be given to the user; otherwise, rewards will be reduced.

Algorithm Running Time: Using this module, we plot the running time of different algorithms.

### C. Architecture Diagram

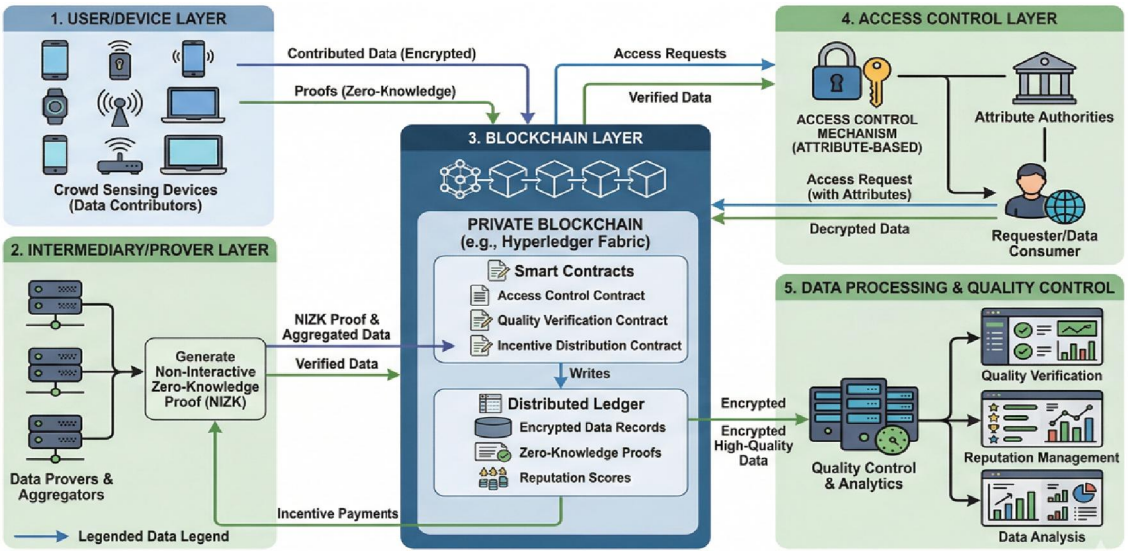


**Fig 3.1: Architecture Diagram of the Proposed PPQC Algorithm**

## IV. RESULTS

### A. Smart Contract Deployment

The Crowd Sensing smart contract is deployed on the Ethereum blockchain with functions to create and get participant block data. The contract address is specified in the Python code to create mobile sensing user blocks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, April 2026
Impact Factor: 8.2

**B. Network Generation**

The simulation generates 20 mobile sensing users (red circles) and one publisher (blue circle). Users are randomly positioned with sufficient distance between them to simulate real-world distribution.

**C. Data Submission and Verification**

When a participant submits data, the system:

Applies Homomorphic privacy preservation to location data

Sends encrypted data to the blockchain server

Calculates noise value by comparing ground truth with received data

Assigns or reduces rewards based on noise threshold

Stores transaction details on the blockchain

**D. Performance Analysis**

The algorithm running time graph compares:

Proposed PPQC (Green line): Privacy-Preserving Quality Control mechanism

Existing PPDA (Blue line): Existing Privacy-Preserving Data Aggregation

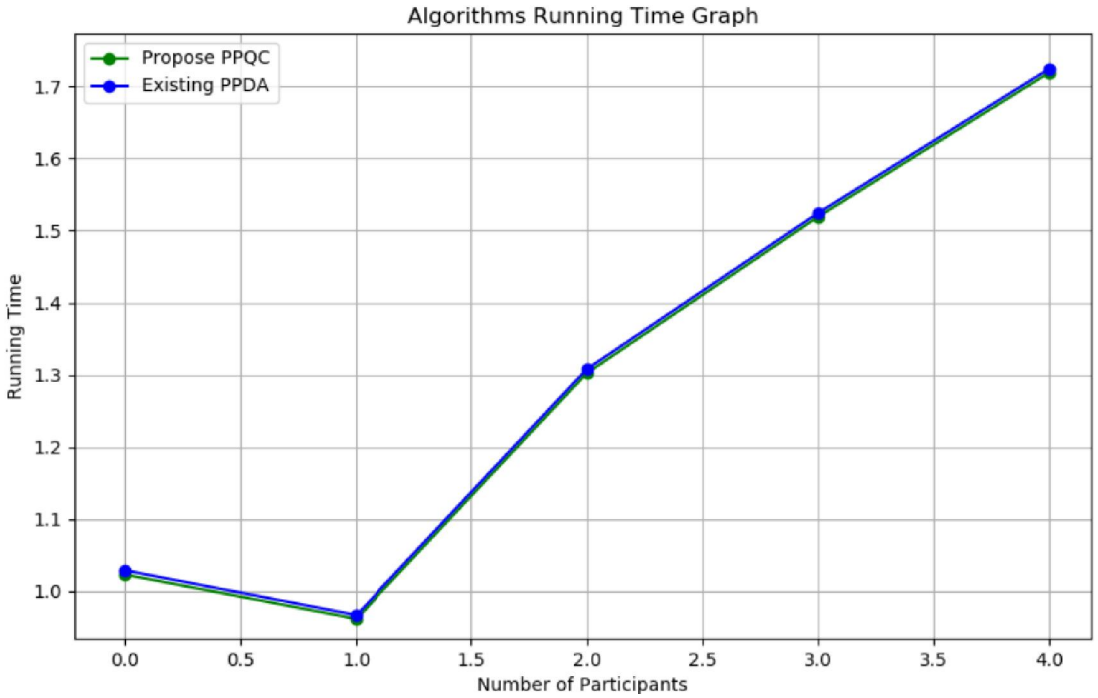


**Fig 4.1 : Graph Representing Running Times of PPDA & PPQC Approaches**

The results show that the proposed PPQC mechanism takes less execution time compared to existing approaches, demonstrating its efficiency while maintaining privacy and security.

## V. CONCLUSION

In this paper, we propose a distributed incentive mechanism based on blockchain which can eliminate the security issues caused by a 'trustful' center. In the distributed crowdsensing system, the sensing data qualities are evaluated via the EM algorithm and contributions are quantified via mutual information by miners. We use a signcryption method to prevent miners and other adversaries from violating users' privacy. The signcryption mechanism saves computing costs compared to operating sequentially of the signature and encryption.


DOI: 10.48175/IJARSCT-32321

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, April 2026 Impact Factor: 8.2

In addition, we use the node cooperation based privacy protection mechanism which makes users' privacy to be hidden in group to deal with the impersonation attacks in the open and transparent blockchain. The experimental results demonstrate that the proposed solution is highly practical and facilitates quality control without violating participant privacy, with improved execution time compared to existing approaches.

In the future, we will analyze the possibility and discuss solutions of collusion attacks between an anonymity group and miners, between miners and the server, and between users and miners.

## REFERENCES

[1] E. K. Kogias P. Jovanovic N. Gailly I. Khoffi L. Gasser B. Ford Enhancing bitcoin security and performance with strong consistency via collective signing Proceedings of the 25th USENIX Security Symposium 279–296.

[2] Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the security and performance of proof of work blockchains. Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 3–16.

[3] Xie, H., Lui, J. C. S., & Towsley, D. (2015). Incentive and reputation mechanisms for online crowdsourcing systems. Proceedings of the IEEE International Workshop on Quality of Service (IWQoS), 207–212.

[4] Peng, D., Wu, F., & Chen, G. (2015). Pay as how well you do: A quality-based incentive mechanism for crowdsensing. Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing, 177–186.

[5] Xiaoqin Gong, Xiaowen Chen, Jing Zhang and Harry Vincent Poor, "Exploiting social trust assisted reciprocity (STAR) toward utility-optimal socially-aware crowdsensing," IEEE Transactions on Signal and Information Processing over Networks, vol. 1, no. 3, pp. 195–208, 2015.

[6] Kumaresan, R., Moran, T., & Bentov, I. (2015). How to use bitcoin to play decentralized poker. Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 195–206.

[7] Luu, L., Teutsch, J., Kulkarni, R., & Saxena, P. (2015). Demystifying incentives in the consensus computer. Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 706–719. [8] Antonopoulos, A. M. (2014). Mastering Bitcoin: Unlocking digital cryptocurrencies. Sebastopol, CA: O'Reilly Media.

[9] Zhang, Y., & van der Schaar, M. (2012). Reputation-based incentive protocols in crowdsourcing applications. Proceedings of the IEEE INFOCOM, 2140–2148.

[10] A incentive-based scheme for mobile sensing Yang, D., Xue, G., Fang, X., & Tang, J. Proceedings of the ACM International Conference on Mobile Computing and Networking, 173–184, 2012.

[11] Ren, X., Yang, J., & Zhang, J. (2012). An improved strategy of preventing privacy inference attacks based on k-anonymity data set. International Journal of Advanced Computer Technology, 4(10), 346–355.

[12] Dent, A. W., & Zheng, Y. (2010). Practical signcryption. Heidelberg: Springer.

[13] Feldman, M., Papadimitriou, C., Chuang, J., & Stoica, I. (2006). Free-riding and whitewashing in peer-to-peer systems. IEEE Journal on Selected Areas in Communications, 24(5), 1010–1019.