Peertechz

ENGINEERING GROUP

TRENDS IN
Computer Science and Information Technology
OPEN ACCESS JOURNAL

ISSN: 2641-3086 DOI: https://dx.doi.org/10.17352/tcsit

Research Article

A Blockchain-based privacy preserving mechanism for mobile crowdsensing

Hilmand Khan*, Hajra Khan, Ayesha Shauqat, Sibgha Tahir, Sarmad Hanif and Hafiz Hamza

Department of Computer Science, COMSATS University Islamabad, Islamabad, Pakistan

Received: 27 January, 2022
Accepted: 09 February, 2022
Published: 11 February, 2022

***Corresponding author:** Hilmand Khan, Masters, Information Security, Department of Computer Science, COMSATS University Islamabad, Pakistan, Tel: +92 336 527 2274; E-mail: hilmand90@gmail.com

Keywords: Privacy; Crowdsensing; Blockchain; Anonymity

https://www.peertechzpublications.com

Check for updates

Abstract

In blockchain-based mobile crowdsensing, reporting of real-time data is stored on a public blockchain in which the address of every user/node is public. Now, the problem lies in the fact that if their addresses get shown to adversaries, all their transactions history is also going to be revealed. Therefore, crowdsensing demands a little privacy preservation strategy in which the identity of a user is unable to be revealed to an adversary or we can say that crowd sensors while reporting the real-time data must provide some level of anonymity to crowdsensing users/nodes [1]. The current crowdsensing architecture is not secure because of its centralized nature and the reason is a single point of failure also numerous kinds of attacks are possible by adversaries such as linkage attacks, Sybil attacks, and DDOS attacks to get the identity or any other valuable information about the nodes. The location of crowd sensors is also a threat that could lead to adversarial attacks. Consequently, some blockchain-based models must be proposed to attain privacy on the blockchain ledger. The solution can either be made up crowdsensing environment on a private blockchain or smart contracts may be the answer to this problem by which we can make the users secure from several attacks conducted by adversaries on the blockchain.

Introduction

Crowdsensing is an enthralling paradigm that refers to geo-crowding in which mobile users utilize their mobile computing, communication, and sensing devices to gather and evaluate information.

Crowdsensing architecture

The architecture of crowdsensing has three units: Service providers, customers, and mobile users. The service providers utilize cloud services to provide crowdsensing services because of having enough storage and resources [2]. They receive tasks about crowdsensing from customers and then assigned those tasks to mobile users. The customers that can be individuals or organizations do not have abilities to perform tasks on their own, so they request service providers for help. Once the tasks are performed, they can obtain the crowdsensing results from service providers.

The collected data is filtered and processed at the servers and delivered to mobile users. The quantity of data collected is uploaded to service providers based on crowdsensing tasks released by customers, varying from general data, such as temperature, air quality, and traffic condition, to more specialized information, such as suggested places and medical conditions.

Now, whether this real-time data from the surroundings is stored on a centralized server there is a possibility that the data will be compromised and leads to the leakage of information. The existing crowdsensing architecture is relying on central servers that are susceptible to attacks such as DoS (Denial of Services), Sybil attacks, etc.

To overcome these security issues, the centralized system of crowdsensing can be replaced with blockchain which is decentralized in nature so it will provide a secure environment to users. Thus blockchain-based crowdsensing will be more secure and immutable. All the data will be kept on a public blockchain, in which nodes can be entered easily and make

Citation: Khan H, Khan H, Shauqat A, Tahir S, Hanif S, et al. (2022) A Blockchain-based privacy preserving mechanism for mobile crowdsensing. Trends Comput Sci Inf Technol 7(1): 001-006. DOI: https://dx.doi.org/10.17352/tcsit.000044

transactions. Every node taking part in the blockchain has the authority to perform read and write operations.

However, with all this development some privacy issues were also raised as there will be full access for each node to do transactions also anyone on the network can send and receive crowdsensing information. So, privacy preservation strategies must be applied for the security and protection of blockchain-based crowdsensing information.

Crowd-sensing phases

Crowdsensing consists of four phases i.e., task allocation, data collection, data analysis, and reward feedback as shown in Figure 1.

Task allocation

A client crowdsources a crowdsensing task to the service supplier, along with the claimed rewards for attracting mobile users and alternative data used to evaluate the task fulfillment [3]. The service supplier accepts the task and assigns it to mobile phone users in line with the task necessities and therefore the profiles of mobile users.

Data collection

Upon receiving the task, mobile users first off verify whether to accept the task or not. If yes, they begin to perform the task by collecting information from their close areas exploiting the onboard sensors, and pre-processing them to produce crowdsensing reports that supported the task demands. Finally, they deliver the reports to the service supplier.

Data analysis

When the service supplier receives decent sensing reports from mobile users, it analyzes the sensing reports by activating many operations, e.g., truth discovery, information statistics, and machine learning, and turn out a crowdsensing result for the client. The client reads the crowdsensing result to get the knowledge and achieve the task

Reward feedback

The client provides feedback concerning the standard of the sensing details, and the service supplier delivers the rewards to the mobile users in compliance with the feedback from the client Table 1.

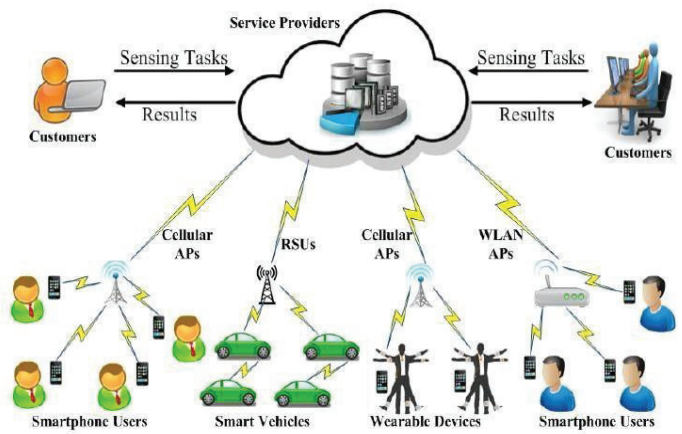

Figure 1: Traditional System Model of Crowdsensing [3].

Table 1: Comparison of anonymity and security in recent research.

Reference number	Anonymity	Security
[17]	✓	✓
[18]	✓	✓
[19]	✓	✓
[20]	✓	✓
[21]	✓	✓
[5]	✓	✓
[21]	✓	✓
[6]	✓	✓
[9]	✓	✓

Related work

In recent years we have noticed that a lot of work has been done in IoT systems, that are based on blockchain due to the advantages blockchain provides, it has been used for security and privacy purposes. However, some privacy-preserving techniques need to be used to ensure privacy on the general ledger and to prevent it from adversaries.

E-cash and bitcoin

[4] introduced Zerocoin, which is a cryptographic extension to Bitcoin which enhances the protocol to consent for entirely anonymous currency transactions [5] endeavor to settle the two major issues which are forward reliable announcements devoid of the disclosure of user's identities and they lack the enthusiasm to forward announcements, by proposing CreditCoin which is an effective announcement network. CreditCoin is considered a unique incentive announcement network based on blockchain which also preserves the privacy of the network.

Privacy and security

[6] proposed an innovative hybrid blockchain crowdsourcing platform which is named by zkCrowd that assimilates with the smart contract and dual consensus protocols to maintain communications and authenticate transactions on the blockchain, and also preserve privacy.

zkCrowd can have the ability to achieve diverse privacy protection for the various crowdsourcing tasks by utilizing smart contracts and zero-knowledge proof as well [7] conceptualize a reliable and privacy-preserving PHI assigning BSPP scheme, which is based on blockchain and is used for diagnosis enhancements in e-Health systems. The proposed protocol has been able to achieve security of data, safe and secure searching, preservation of privacy. They employed the proposed scheme on 'JUICE' and weigh up the accomplishment beginning with the characteristics of storage, communication, and time overhead as well.

The conventional centralized crowdsourcing system has many problems such as disclosure of privacy and single point of failure also have services with high fees [8], to overcome the above-mentioned issues of centralized system Ming Li

Citation: Khan H, Khan H, Shauqat A, Tahir S, Hanif S, et al. (2022) A Blockchain-based privacy preserving mechanism for mobile crowdsensing. Trends Comput Sci Inf Technol 7(1): 001-006. DOI: https://dx.doi.org/10.17352/tcsit.000044

[9] anticipated an agenda for crowdsourcing called CrowdBC which is based on blockchain and also decentralized. In the suggested framework a client's task could be resolved by a crowd of manual workers without having to rely upon some third-party involvement. This scheme is more linked to our work for privacy-preserving mechanisms for blockchain-based crowdsensing.

Encryption and differential privacy

In order to ensure the protection of data and preserve its privacy Differential privacy (DP) and Encryption are being used [10]. Distributed architectures are intended to thwart just one single point of failure and bottleneck problems. Nevertheless, several of that research square measures plotted on the normal triangular structure crowdsensing models that have suffered from the collapse of trust [11] proposed a Differentially Private Double Auction with Reliability-Aware in Mobile Crowdsensing (DPDR). Specifically, the authors designed the incentive mechanism by using the exponential mechanism in double side auctions for the selection of clearing price tuples. Moreover, in order to be able to collect accurate sensory data, more unfailing workers were chosen heuristically as candidates for each clearing price tuple Table 2 [12] designed novel privacy-preserving mechanisms for users' true bid information protection against the honest but curious platform and minimizing the social cost of the winner selection. In the scheme, a differential privacy bid obfuscator is designed, rather than uploading true bids on the platform, which enables the users to obfuscate their bids locally and submit obfuscated bids to the platform [13] surveyed comprehensively privacy-preserving mechanism for the protection of location privacy of workers and compared them according to different parameters. The authors divided the mechanisms into three categories according to the nature of their algorithms and compared them from the architecture viewpoint, privacy, and computational overhead. Up to now, none of the active works has solved every bit of the mentioned problems at the very same time.

Blockchain-based crowd-sensing system

[14] and [15] stated blockchain-based crowdfunding which is crowd-sourced [16] elicited an alternative protocol that uses blockchain headed for confronting the problem of small-value transactions in crowdsensing. Besides, the study working on crowdsourcing built on the blockchain has additionally earned significant implications in the industry lately, such as microwork.

The above-stated mechanisms are inadequate to their explicit applications, but our goal is wider and covering all the characteristics that we are trying to resolve with our proposed mechanism because we hypothesized a decentralized framework for crowdsensing which is obviously based on blockchain which means that it does not be contingent on some central third party to varnish the process of crowdsourcing and pledges privacy through permitting nodes to register without identity which can efficiently astonish many attacks on blockchain offering full protection to the crowdsensing users on the blockchain. Moreover, users on the blockchain do not require to pay the pricey maintenance fees to conventional crowdsensing policy anymore, simply that it is necessary to give a small number of transaction costs. The anticipated framework for blockchain-based crowdsensing will also enhance the essential flexibility of crowdsensing.

Methodology

In this segment, we will discuss the proposed mechanism for privacy-preserving blockchain-based crowdsensing. The mechanism will consist of five entities which namely are workers who receive the tasks and on successful completion, the reward will be given to them, requesters who post the tasks on the blockchain while the crowdsensing client act as a medium between workers and requesters, at the end all the transactions are being stored on the blockchain Figure 2.

The system model for this work consists of a few units which can have been named as requesters that could be identified by R= {R_1, R_2,... R_n}. Requesters posts a task on the service provider that is a decentralized server. The workers W= {W_1, W_2,... W_n}. on the system is identified as the community that competes for the tasks, they have skills and can perform the posted tasks on the system by requesters. There is another

Table 2: Outline of Blockchain-based Privacy Mechanism in Recent Research.

Ref no	Tools	Architecture	Mechanism	Limitation	Key Contribution	Privacy Enhancement
[16]	N/A	Distributed	Bilinear pairing	Certain nodes suffering from cyber attacks	Information safety & confidentiality	1)Patient's identity 2)Location of change
[17]	N/A	Partially Centralized	BSPP for consortium blockchain	Storage and Communication overhead	Searchable data confidentiality	1)Patient's original identity
[19]	ZK-Snark	Decentralized	ZeroCash	Hampering accountability, regulation, and oversight	Prevent public transaction leakage	1)User identity
[20]	Mirac l	Partially Centralized	FICA	Computational Costs	Data encryption Conditionally anonymous traceability protection	1)Traceability 2)Auditability
[5]	PolarSS L, GMP	Decentralized / Distributed	CreditCoin	Key Management & Coin Balance	Unnamed announcement in a non-confidential environment	1)Vehicular identity
[6]	RSA, TCA, DPOS consens us, ZK-SNARK	Decentralized	zkCrowd	Performance Improvement	Elevated transaction throughput Diverse privacy protection Resistance to severe attacks	1)Verify transactions and preserve privacy
[9]	URC and RWR C Contra ct Ropsten, javascript ipt	Distributed/ Decentralized	CrowdBC	Efficient Evaluation	Fully Fraud Resilient Augmented the flexibility of crowdsourcing by smart contract	1)Pseudonymity 2)Trust worthy Worker Selection

Citation: Khan H, Khan H, Shauqat A, Tahir S, Hanif S, et al. (2022) A Blockchain-based privacy preserving mechanism for mobile crowdsensing. Trends Comput Sci Inf Technol 7(1): 001-006. DOI: https://dx.doi.org/10.17352/tcsit.000044

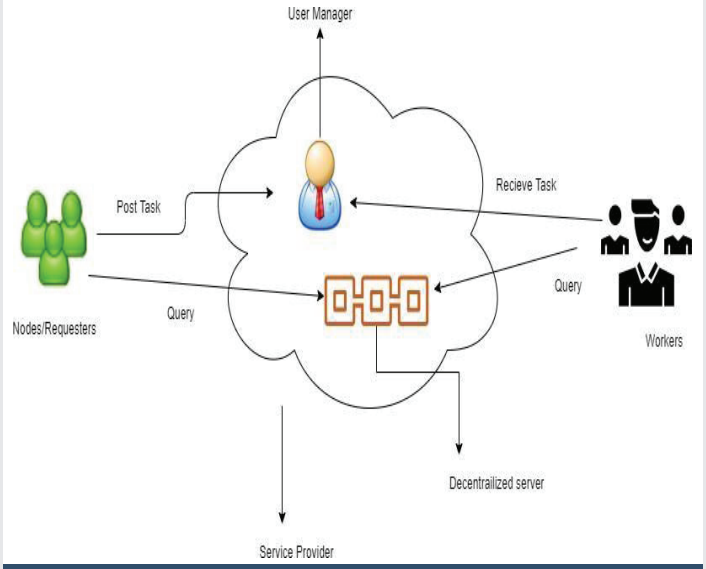

Figure 2: Block chain-based.

entity which is called a crowdsensing client, which acts as a medium for both R and W. This is not based on any third- party. All the actions performed on the medium are transmitted to the storage.

Proposed mechanism

1) Registration

a. A new user sends a request to the registration unit for registration.

b. The registration unit forwards this request to the blockchain.

c. Blockchain receives the request and makes sure that this user has not registered already, for the registration to proceed, the blockchain requests for the user data.

d. The user sends his/her public key as an authentication parameter.

e. The registration system validates this parameter and upon validation, this parameter is sent to the blockchain.

f. Blockchain saves this data.

g. A Username UID and password PWD are sent to the user.

2) Login

1) The user starts a connection with the login service.

2) The system requests the username UID and passwords PWD of the user.

3) The user enters his/her credentials and transmits them to the login service.

4) The login service checks and sends the data to the blockchain.

5) The blockchain validates the credentials and sends an "OK" signal to the login service.

6) The login service grants access to the user Figure 3.

3) Updating

The workers that are already registered on the blockchain receive the task posted by the requesters by interacting with the crowdsensing client. Once the workers complete the allocated task before the deadline, they sent it to the storage. The solution they provided for the task is encrypted with the public key of the requester.

4) Reward assignment

This is the last step of the process in which a reward is given to the registered workers on the successful completion of the given task. The reputation of those workers will be improved who have done high efforts and given good performance for the completion of the task.

Protocol analysis

The following analysis has been done in terms of security objectives with the proposed mechanism.

- No malicious user can modify the data. Integrity is being maintained using blockchain.
- The registration system is preventing malicious user entrance into the system, as a result maintaining the privacy of the user.
- Only the users registered in the system can participate in the system. No un-authenticated user can access the system.
- The crowdsensing data being maintained in the system maintains confidentiality using blockchain.
- Multiple entities in decentralized locations can build trust and consensus in one place.

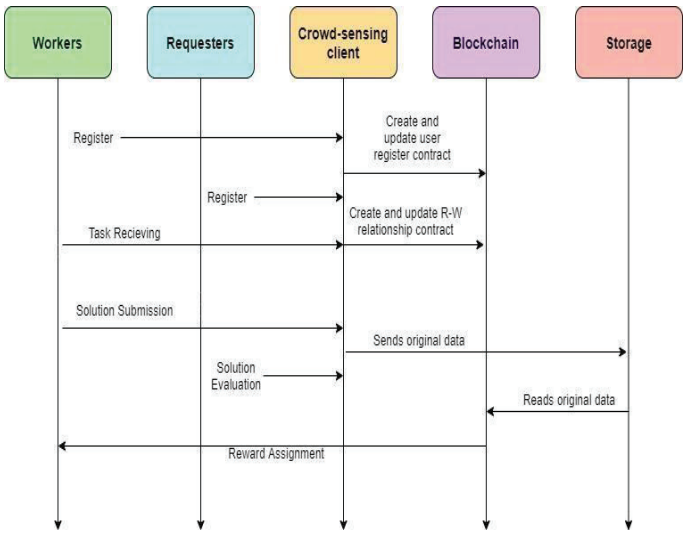

Figure 3: The process of smart contract updating on blockchain.

Citation: Khan H, Khan H, Shauqat A, Tahir S, Hanif S, et al. (2022) A Blockchain-based privacy preserving mechanism for mobile crowdsensing. Trends Comput Sci Inf Technol 7(1): 001-006. DOI: https://dx.doi.org/10.17352/tcsit.000044

Experimental setup

As we discussed earlier in the above section that privacy for the crowdsensing on the blockchain can be preserved by using smart contracts. So, for the implementation of smart contracts, we have used Ethereum blockchain as a private network and compiled the smart contract code on solidity ("https://solidity.readthedocs.io/en/develop/"), which allows us to make smart contracts with public and private methods also providing a set of basic data types, it is developed only for smart contracts creation. The complied program to Ethereum virtual machine (runtime environment for smart contracts which is built on Ethereum) code on the Ethereum blockchain can be deployed as a smart contract. The compiler of solidity converts code into EVM bytecode, the bytecode is redirected to the Ethereum network as a deployment transaction. In the EVM, gas is a measurement unit applied for assigning fees to each transaction with a smart contract.

The gas can be used to calculate the transaction fee given as, Transaction fee = Total gas used*gas price. The complexity of computations is directly proportional to the gas, the more complex the computations are, the higher will be its gas value required to run a smart contract.

The implementation of smart contracts on solidity is explained step by step as followed.

1) Enabling metamask chrome extension

This is the first step before writing any smart contract. Enable MetaMask on chrome browser, which allows a user to interact with smart contracts on the web without downloading the blockchain. It acts as a wallet also as an Ethereum blockchain. Enable the extension in chrome and then create a wallet then proceed to the submission of Ether. The user must have some number of ethers to deploy a smart contract on the network of Ethereum blockchain.

2) Choosing any test network

A list of networks will be displayed, we chose the Robsten Test Network mentioned in the list. The ether added here has no real value, these are dummy ethers for testing the smart contracts.

3) Using Solidity for writing Smart Contracts

The others are added to the wallet which means that now we can write the code for smart contracts.

4) Deploy the Smart Contract

Create a file with .sol extension and place the code of the ERC20 token which will store in the user wallet that is deploying the smart contract. Now go to MetaMask enter the address of the smart contract and the number of tokens will be shown Table 3.

Results

Here in this section, we will discuss the result generated results of smart contracts on solidity. There is no need for the explicit sender as (msg. sender) is already available in the function body on solidity. In the proposed mechanism for preserving privacy on the Ethereum blockchain, the user can create an account or change its ID regularly for each implementation of a smart contract so that it can not be tracked by the adversaries.

The data types that are being used in the executed smart contract on solidity are uint (a 256-bit unsigned integer type used to store distance values), bytes32 (an array of 32 bytes which is used to store the output of a cryptographic hash function), string (a character array used to pass error messages in function return values) and address (a special data type used to store the address of a message caller).

For a block 8112742 having transaction (txn) hash 0x2d0405e5eb113a33f9557023b6bbfa660ed11bc6baff02e2139df863b4775716 and address 0xbbf5029fd710d227630c8b7d338051b8e76d50b3 a smart contract is deployed on the Ethereum blockchain. The transaction fee remains the same in all cases i.e., 0.00021 ethers.

S.No.	Limitations Identified	Desired Outcome
1	Privacy Preservation	✓
2	Linkage attack	✓
3	Sybil attack	✓
4	DDOS	✓
5	Workers' Reward	✓

Conclusion

In this paper, we proposed a blockchain-based privacy-preserving mechanism in crowdsensing, while protecting the system against linkage attack, Sybil attack, and DDOS by using blockchain and introducing a reward mechanism for tasks completion. Moreover, The scheme deals with privacy

Table 3: Overview of Result for the Proposed Mechanism.

Ref no	Block Height	Transactions	Block Reward	Difficulty	Size	Gas Used	Gas Limit	Nonce
1.	8112742	23 transactions and 80 contract internal transactions in this block	2.148164864 Ether (2+0.148164864)	1,121,717,100	28,525 bytes	7,739,434 (96.74%)	8,000,029	0xb416d13006150323
2.	8112727	32 transactions and 81 contract internal transactions in this block	2.069562673 Ether (2+0.069562673)	1,116,799,963	6,706 bytes	4,886,507 (61.08%)	8,000,029	0x651e28f4057e0ebb
3.	8112741	5 transactions and 8 contract internal transactions in this block	2.083806446 Ether (2+0.083806446)	1,121,169,654	7,098 bytes	2,409,627 (30.12%)	8,000,029	0x54ca50d0d3103b43

Citation: Khan H, Khan H, Shauqat A, Tahir S, Hanif S, et al. (2022) A Blockchain-based privacy preserving mechanism for mobile crowdsensing. Trends Comput Sci Inf Technol 7(1): 001-006. DOI: https://dx.doi.org/10.17352/tcsit.000044

preservation and secures transaction data from being available publicly. The proposed framework although handled the issues of centralized servers but due to the high cost of operation and lack of privacy by design it might be possible but not feasible to implement a privacy-preserving protocol on Ethereum blockchain tapping smart contracts. So, the cost for deploying smart contracts on Ethereum blockchain must be below for future research on maintaining the privacy of smart contracts for any purpose in blockchain technology.

References

1. Ul Hassan M, Rehmani MH, Chen J (2019) Privacy Preservation in Blockchain-Based IoT Systems: Integration Issues, Prospects, Challenges, and Future Research Directions. Future Gen Compu Syst 97: 512-529. **Link:** https://bit.ly/3HIMEBV
2. Zhuo G, Jia Q, Guo L, Li M, Li P (2017) Privacy- Preserving Verifiable Set Operation in Big Data for Cloud- Assisted Mobile Crowdsourcing. IEEE Internet Things J 4: 572-582. **Link:** https://bit.ly/3uxTGpr
3. Kim JW, Edemacu K, Jang B (2022) Privacy-preserving mechanisms for location privacy in mobile crowdsensing: A survey. J Netw Comput Appl 200: 103315. **Link:** https://bit.ly/3LlgcIc
4. Miers I, Garman C, Green M, Rubin AD (2013) Zerocoin: Anonymous Distributed E-Cash from Bitcoin. 2013 IEEE Symposium on Security and Privacy, Berkeley, CA 397-411. **Link:** https://bit.ly/3gyMnFL
5. Li L, Liu J, Cheng L, Qiu S, Wang W, et al. (2018) CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles. IEEE trans Intell Transp Syst 19: 2204-2220. **Link:** https://bit.ly/3uRCHPd
6. Zhu S, Li W, Cai Z, Hu H, Li Y (2020) zkCrowd: A Hybrid Blockchain-Based Crowdsourcing Platform. IEEE Trans Industr Inform 16: 4196-4205. **Link:** https://bit.ly/35O3rFx
7. Yang K, Zhang K, Ren J, Shen X (2015) Security and privacy in mobile crowdsourcing networks: challenges and opportunities. IEEE Commun Mag 53: 75-81. **Link:** https://bit.ly/35PTIP2
8. Buddhadeb H (2017) Crowdsourcing crisis management platforms: a privacy and data protection risk assessment and recommendations. **Link:** https://bit.ly/3LoyvMn
9. Li M, Weng J, Yang A, Lu W, Zhang Y, et al. (2019) CrowdBC: A Blockchain-Based Decentralized Framework for Crowdsourcing. IEEE Trans Parallel Distrib Syst 30: 1251-1266. **Link:** https://bit.ly/3HGqoZn
10. To H, Ghinita G, Fan L, Shahabi C (2017) Differentially Private Location Protection for Worker Datasets in Spatial Crowdsourcing. IEEE Trans Mob Comput 16: 934-949. **Link:** https://bit.ly/3LnBzZm
11. Ni T, Chen Z, Xu G, Zhang S, Zhong H (2021) Differentially private double auction with reliability-aware in mobile crowd sensing. Ad Hoc Networks 114: 102450. **Link:** https://bit.ly/3GDBsp1
12. Wang Z, Li J, Hu J, Ren J, Wang Q, et al. (2021) Towards privacy-driven truthful incentives for mobile crowdsensing under untrusted platform. IEEE Trans Mob Comput. **Link:** https://bit.ly/34l7okZ
13. Li Z, Liu J, Hao J, Wang H, Xian M (2020) CrowdSFL: A Secure Crowd Computing Framework Based on Blockchain and Federated Learning. MDPI. **Link:** https://bit.ly/3spUkCJ
14. García VJ, Calvo A, Hassan S, Sánchez-Ruiz AA (2016) Betfunding: A distributed bounty- based crowdfunding platform over ethereum. Distributed Computing and Artificial Intelligence, 13th International Conference 403-411. **Link:** https://bit.ly/3uCBrPF
15. Zhu H, Zhou ZZ (2016) Analysis and outlook of applications of blockchain technology to equity crowdfunding in China. Finance Innov 2: 29. **Link:** https://bit.ly/3gAnTfm
16. Buccafurri F, Lax G, Nicolazzo S, Nocera A (2017) Tweetchain: An Alternative to Blockchain for Crowd-Based Applications. ICWE. **Link:** https://bit.ly/3oClmpj
17. Wu HT, Tsai C (2018) Toward Blockchains for Health-Care Systems: Applying the Bilinear Pairing Technology to Ensure Privacy Protection and Accuracy in Data Sharing. IEEE Consum Electron Mag 7: 65-71. **Link:** https://bit.ly/364VtZ3
18. Zhang A, Lin X (2018) Towards Secure and Privacy-Preserving Data Sharing in e- Health Systems via Consortium Blockchain. J Med Syst 42: 140. **Link:** https://bit.ly/3gBW46p
19. Shetty S, Kamhoua CA, Njilla LL (2019) Blockchain for Distributed Systems Security. 352. **Link:** https://bit.ly/3uxTzdv
20. Li M, Zhu L, Lin X (2020) Efficient and Privacy-Preserving Carpooling Using Blockchain- Assisted Vehicular Fog Computing. IEEE Internet Things J 1. **Link:** https://bit.ly/3rBQO9d
21. Svetinovic D (2018) Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. IEEE Trans Dependable Secure Comput 15: 840- 852.
22. Nakamoto S (2020) Bitcoin: A Peer-to-Peer Electronic Cash System. **Link:** https://bitcoin.org/bitcoin.pdf
23. Alsheikh MA, Jiao Y, Niyato D, Wang P, Leong D, et al. (2017) The Accuracy-Privacy Tradeoff of Mobile Crowdsensing. IEEE Commun Mag 55. **Link:** https://bit.ly/34HbYJW

Citation: Khan H, Khan H, Shauqat A, Tahir S, Hanif S, et al. (2022) A Blockchain-based privacy preserving mechanism for mobile crowdsensing. Trends Comput Sci Inf Technol 7(1): 001-006. DOI: https://dx.doi.org/10.17352/tcsit.000044