Blockchain-based Crowd-sensing System

Junqin Huang, Lingkun Kong, Linghe Kong*, Zhen Liu, Zhiqiang Liu and Guihai Chen
Shanghai Key Laboratory of Scalable Computing and Systems, Shanghai Jiao Tong University, China
*Corresponding Author
junqinhuang95@gmail.com, {klk316980786, linghe.kong}@sjtu.edu.cn, {liuzhen, liu-zq, gchen}@cs.sjtu.edu.cn

***Abstract*—Crowd-sensing systems have gained considerable interests and adoption in recent years. However, most existing crowd-sensing systems rely on central servers, which are subject to low reliability due to the traditional centralized architecture and high service fee. Motivated by constructing a crowd-sensing system with security and low service fee, we propose a blockchain-based crowd-sensing system (BCS), which replaces traditional triangle architecture by decentralized blockchain system. Also, in order to accelerate the formation of the fabric of trust, BCS implements applications of smart contracts to reward sensing-task workers, which offers reliable anonymity in the meantime. By leveraging blockchain technology, BCS has good performance in privacy protection and system robustness.**

***Index Terms*—Blockchain, crowd-sensing, smart contract, decentralization, security**

I. Introduction

As we know, the traditional centralized architecture of crowd-sensing systems may lead to privacy leakage and single point of failure [1]. They are also vulnerable to distributed denial of service (DDoS) and Sybil attacks due to malicious users involvement [2]. In addition, high service fee charged by the crowd-sensing platform which has monopolized the market may stem the development of crowd-sensing. So how to address these potential issues remains to be an open problem.

There have been several studies to deal with part of the aforementioned open problem [3]–[5], while the majority of these researches are built on the traditional triangular structure crowd-sensing models, which suffer from breakdown of trust. With the emergence of blockchain and its multiple applications [6]–[8], solving all of the above issues in crowd-sensing systems becomes possible. However, in the context of blockchain applications, current prevalent blockchain-based systems such as Bitcoin [6], Litecoin, Zcash [8], etc., always issue virtual currencies to incentivize miners which is hard to format the fabric of trust.

To tackle above challenges, we propose a blockchain-based decentralized crowd-sensing system (BCS), in order to alleviate privacy leakage and reduce the charge of the central platform. The service fee charged by platform can be used more efficiently, as it now is all paid to sensing-task workers and blockchain miners instead of central crowd-sensing platforms. Since the methods of getting rewards are substantiated by published smart contract, both requesters and workers can trust the immutable codes from published smart contract as a credible administrator. Therefore, BCS can also quickly establish the fabric of trust among users. Our main contributions are listed as follows:

978-1-5386-4870-4/18/$31.00 ©2018 IEEE

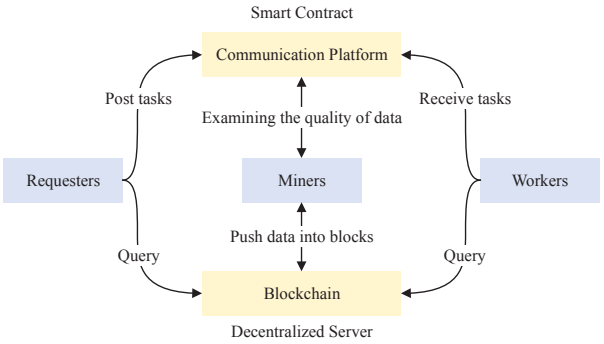

Fig. 1. The architecture and crowd-sensing process of BCS.

- We propose a crowd-sensing system based on blockchain, which can eliminate the security and privacy issues well.
- We implement BCS based on Ethereum, which verify the feasibility and effectiveness of our proposed system.
- Further theoretical analysis and experiments demonstrate the security and efficiency of BCS.

II. Blockchain-based Crowd-sensing System

Diffrent from the traditional architecture, in the blockchain-based decentralized system, there is no centralized platform in crowd-sensing process. Instead, by leveraging blockchain technique, the crowd-sensing process is managed by a decentralized system, which is shown in Fig.1.

From Fig.1, we know that BCS consists of five groups of roles: Requesters, Workers, Miners, Blockchain, Communication Platform. And the crowd-sensing process of BCS can be divided into following four steps:

1) Requesters post tasks, then initialize the examining rules and send them to communication platform, i.e., publish a smart contract that consists of several predefined functions.
2) Workers query published smart contracts from blockchain and obtain attractive sensing tasks. After completing tasks by recording sensing data, they post the data to communication platform, i.e., call specific functions in smart contracts.
3) By querying blockchain and listening to the communication platform, miners fetch unsubstantiated sensing data, and then examine the quality of data according to rules the requester makes. After miners substantiate the quality of sensing data, miners and workers will get the rewards after pushing processed sensing data into blocks. In general, miners obtain rewards by contributing computing power for running smart contracts.
4) Requesters listen to the blockchain periodically. Once they

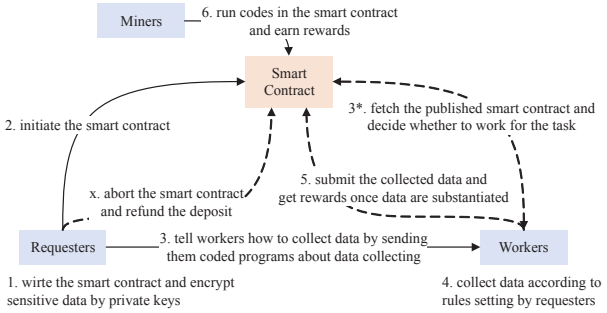

Fig. 2. The crowd-sensing process of BCS after adding smart contracts.

decide not to continue collecting data, they can send message to the system to close this task and get the remained reserve money from smart contract. As this message will be broadcasted in the system, miners and workers will then cease to work.

More specifically, requesters create smart contracts by setting requirements for sensing data and store a certain amount of deposits for determining the rewards. After that, once workers are attracted by the rewards as well as their data are substantiated by miners, they can get rewards stored in the smart contract protocol right away. That is to say once they get works done, they can receive valuable rewards. Therefore, the reputation of this system can be quickly built, and the enthusiasm of both miners and workers can be aroused.

III. Detailed Implementation of Smart Contract

After learning about the architecture and crowd-sensing process of BCS, in this section, we use a specific case (i.e., WiFi-sensing task) to show how it works. Fig.2 shows that the structure of BCS after adding a specific smart contract.

In Fig.2, we illustrate the detailed process of the system. The number indicates the order of the operation in a certain crowd-sensing task, where operation 3* means this operation can be processed concurrently with operation 3, and operation x means this operation can be undertaken in any time after operation 2. Moreover, the solid lines in Fig.2 stand for operations being necessarily done in a certain task, while the dashed lines indicate these operations might not be executed.

For the example of WiFi-sensing task, requesters publish the smart contract and initiate rules of the WiFi-sensing task, and workers can choose whether to receive this task depends on how attractive of its rewards. We can implement the smart contract of WiFi-sensing task according to Fig.2. Due to limited space, the source code of smart contract and the interfaces of the WiFi-sensing task has been published on the webpage: https://github.com/Ohyoukillkenny/BCS.

IV. Experiments and Analysis

A. Financial Efficiency

It's obvious that the minimum cost of requesters for each data largely depends on the cost of transaction fee workers need to pay. In this section, using the WiFi-sensing task as an instance, we count the average cost of transaction fees workers need to pay by lauching experiments of the participation of 1000 workers. The result shows each worker need to pay 0.00052 ETH on average. We use the exchange rate between USD and ETH on 04/11/2018 to roughly estimate the value of 0.00052 ETH as 0.217 USD, which means that requesters need to pay each WiFi-sensing data for at least 0.217 USD.

This value might be too high for a simple WiFi-sensing task. However, when the data the requester attempts to collect are sensitive and require high anonymity (e.g., personal income, medical history), this price might be totally acceptable.

B. Security Analysis

Privacy protection. For the sake of properties of blockchain, we can guarantee privacy by allowing users to register without true identity and storing encrypted sensory data in the distributed database.

System robustness. Because of decentralized architecture of blockchain, BCS does not depend on any central third-party, there is no single point of failure issue. Also, workers actually need to make security deposits, i.e., pay transaction fees to miners, before participation in crowd-sensing task, which efficiently prevents various attacks (e.g. DDoS, Sybil and 'false-reporting' attacks [9]).

Conclusion

We propose a blockchain-based crowd-sensing system (BCS) to make up for the paucity of traditional crowd-sensing systems with security and low service fee in this paper. Since we are still in the early stage of blockchain technology, this project will be of importance to research in distributed systems by providing a concrete blockchain-based solution for a known scientific problem, i.e., crowd-sensing management.

Acknowledgments

This work is partly supported by NSFC (61672349, 61672353, 61472252), National Key Research and Development Program grant 2016YFE0100600, and China 973 project (2014CB340303).

References

[1] Pournajaf, Layla, et al. "A survey on privacy in mobile crowd sensing task management." Dept. Math. Comput. Sci., Emory Univ., Atlanta, GA, USA, Tech. Rep. TR-2014-002 (2014).

[2] Krontiris, Ioannis, Marc Langheinrich, and Katie Shilton. "Trust and privacy in mobile experience sharing: future challenges and avenues for research." IEEE Communications Magazine 52.8 (2014): 50-55.

[3] Cardone, Giuseppe, et al. "The participact mobile crowd sensing living lab: The testbed for smart cities." IEEE Communications Magazine 52.10 (2014): 78-85.

[4] Hamm, Jihun, et al. "Crowd-ml: A privacy-preserving learning framework for a crowd of smart devices." Distributed Computing Systems (ICDCS), 2015 IEEE 35th International Conference on. IEEE, 2015.

[5] Han, Guangjie, et al. "HySense: A hybrid mobile crowdsensing framework for sensing opportunities compensation under dynamic coverage constraint." IEEE Communications Magazine 55.3 (2017): 93-99.

[6] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[7] Swan, Melanie. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.", 2015.

[8] Greenberg, Andy. "Zcash, an untraceable bitcoin alternative, launches in alpha." (2016).

[9] Zhang, Xiang, et al. "Keep your promise: Mechanism design against free-riding and false-reporting in crowdsourcing." IEEE Internet of Things Journal 2.6 (2015): 562-572.