Research Proposal

Lingkun Kong (klk316980786@sjtu.edu.cn)

Abstract

Motivated by constructing a crowd-sensing system with reliability, security and low services fee, I propose building a blockchain-based crowd-sensing framework that replaces traditional triangle architecture by decentralized blockchain system. Also, in order to accelerate the formation of the fabric of trust, instead of releasing a new virtual currency, the proposed framework implements applications of smart contracts to reward sensing-task workers. Also, by leveraging blockchain technology in crowd-sensing, the proposed framework is also an exploration on the mining puzzles of proof-of-usefulness.

1. Background and Motivation

Crowd-sensing systems, which take advantage of pervasive mobile devices to efficiently collect data, have gained considerable interest and adoption in recent years [1][2]. However, the majority of existing crowd-sensing systems rely on central servers, which are subject to the weaknesses of the traditional trust-based model, such as single point of failure and privacy disclosure [3][4]. They are also vulnerable to distributed denial of service (DDoS) and Sybil attacks due to malicious users' involvement [5]. In addition, high service fees charged by the crowd-sensing platform may stem the development of crowd-sensing. 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 [6-10], while the majority of these researches are built on the traditional triangular structure crowd-sensing models, which suffer from breakdown of trust. Thus, this research proposal is motivated by this: *Can we design a decentralized crowd-sensing system with reliability, security, and low services fee*?

2. Introduction of Proposal

The past few years have witnessed the emergence of blockchain as well as its multiple applications [11,12,16,17,19,22], which provides us an opportunity to solve all of the above issues in crowd-sensing systems simultaneously. Therefore, I propose building **a blockchain-based decentralized framework for crowd-sensing,** with the purpose of alleviating privacy leakage and reducing the charge of the central platform.

To illustrate, by leveraging blockchain architecture, we can replace the centralized crowd-sensing platform by decentralized blockchain system. Therefore, the services fee charged by

the platform can be used more efficiently, as it now is all paid to workers and blockchain miners [14]. Also, since now the crowd-sensing process does not depend on any central third party, there is no single point of failure issue.

Besides, 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. Further, by stipulating that each identity must make a deposit before participation in smart contract protocols, we can efficiently prevent various attacks (e.g. DDoS, Sybil and “false-reporting” attacks [13]).

In the context of blockchain applications, current prevalent blockchain-based systems such as Bitcoin [11], Litecoin [16], and Zcash [17], etc., always issue virtual currencies to incentivize miners and try to convince both miners and users that the virtual currency is worthy of being hold. However, to earn the trust from users and maintain the fabric of trust are quite difficult. Also, legal problems always ensue the issue of virtual currencies, and Governments worry about the high anonymity in currency systems will found the breeding ground for the crime [18]. When dealing with crowd-sensing problems, it is unrealistic to quickly build the reputation of the system and win the trust from users by issuing new virtual currencies. Additionally, with the awareness of legal issues, it is impractical to universally apply systems which release the virtual currency.

Moreover, in traditional blockchain-based systems, there's a concern that Bitcoin mining is extremely profligate, since massive energy is wasted by miners in solving "useless" puzzles for block discovery [21]. Thus, "*Is there a puzzle, whose solution provides useful benefit to society, while still satisfying the basic requirements of Blockchain puzzles?*" is raised to be a natural question. There have been several studies which attempted to reduce blockchain-based system's energy waste, such as Primecoin and Permacoin [19,22]. However, their methods are not feasible for a lot of potential candidates such as problems of protein folding [23], space signal searching [20], which are of great scientific usefulness while needs a trusted administrator. In this case, building a blockchain-based crowd-sensing framework will also be an exploration of the proof-of-usefulness puzzle, which might be helpful to reduce the energy waste in traditional blockchain systems.

Faced with these challenges, in my proposed framework, I introduce applications of smart contracts to reward users, which should be first initiated by sensing-task requesters with certain reserve money. On the one hand, by this method, we can build the reputation of the framework and raise the enthusiasm of both miners and workers in a short time. On the other hand, since there is deposit in the smart contract and users can directly receive

rewards from smart contract once their works are substantiated in blockchain, both workers and miners can trust the requester as a credible administrator whose reputation is authorized by bank. Therefore, the new framework will be feasible for broad implementation of proof-of-usefulness puzzles.

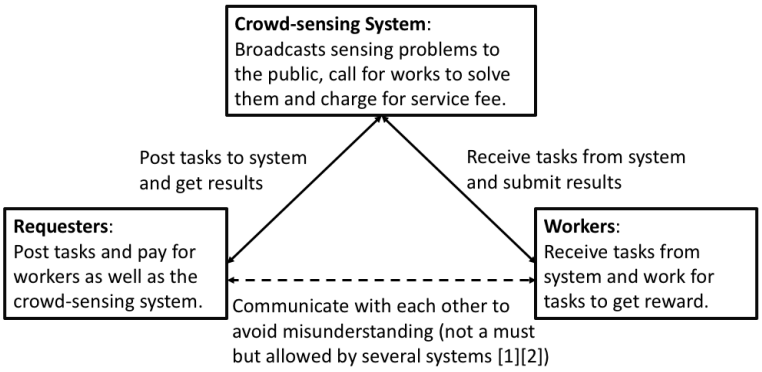

Fig 1. The system model of traditional crowd-sensing.

3. Basic Design and Methods

The traditional crowd-sensing process consists of three groups of roles: requesters, workers and a centralized crowd-sensing system, where requesters submit tasks to the system and receive sensing results from the system; workers pull tasks from the system, complete tasks they interested in and submit sensing results to the system; the centralized system deals with submissions from requesters and workers and responds them accordingly. Figure 1 presents the crowd-sensing by traditional centralized systems.

In the blockchain-based decentralized system which I propose, there is no centralized platform in crowd-sensing process anymore. Instead, by leveraging blockchain and P2P network, the crowd-sensing process is managed by a decentralized system, which is presented in Figure 2.

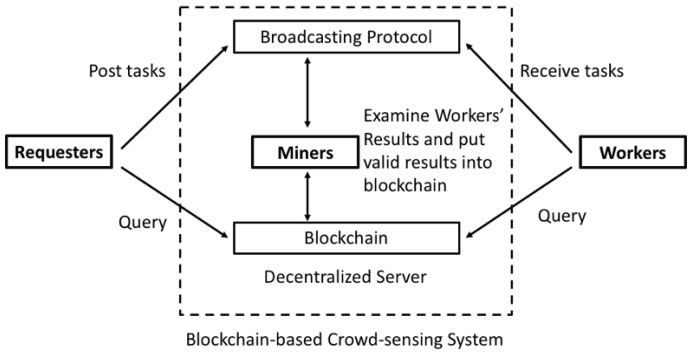

Fig 2. The system model of blockchain-based crowd-sensing process.

Basically, the crowd-sensing process can be divided into following steps:

Step1: Requesters broadcast tasks, and, meanwhile, they need to initialize the *examining rules* as well as the *smart contract parameters* by delivering parameters to system interface.

Examining rules: Examining rules stipulate the examination of the sensing data. Actually, crowd-sensing always encounters a bunch of noisy, low-quality data [3]; while further inspection is always arduous for requesters. Therefore, I propose that miners take the inspection work as part of puzzles they need to solve to discover a new block. Technically, requesters set up the mining rules by downloading a program from system and generate a **black box** for miners, which we will discuss later in the section about black box.

Smart contract parameters: The smart contract parameters contain the initial reserve money requesters put in smart contract, and they stipulate how do miners and workers share the rewards, as the new found block contains the fruit of labor from both miners and workers.

Step2: Workers, by querying blockchain and fetching message from broadcasting protocol, obtain attractive sensing tasks. After finishing tasks by recording sensing data, they save these data in local devices and then post the message to task managing interface including data address and information about their identities.

Step3: By querying blockchain and listening to broadcasting protocol, miners fetch unsubstantiated sensing data from workers' local devices, and they can examine the quality of this data based on rules the requester establishes. After miners substantiate the quality of sensing data, they will attempt to solve hash puzzle to integrate these data into a block, which will be later added to blockchain. Then, miners and workers can share the rewards of the block.

Step4: Requesters listen to the blockchain periodically. Once they are satisfied with sensed data or decide to not continue collecting data for other reasons, they can send message to the system to burn the blockchain 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.

4. Introduction of Smart Contract

Additionally, I propose to add applications of smart contracts over the whole framework with the purpose of quickly obtaining users' trust and making the design feasible for various purposes, such as aforementioned problems of protein folding and aliens discovery. Figure 3 shows the relationship between the smart contract protocols and the decentralized system.

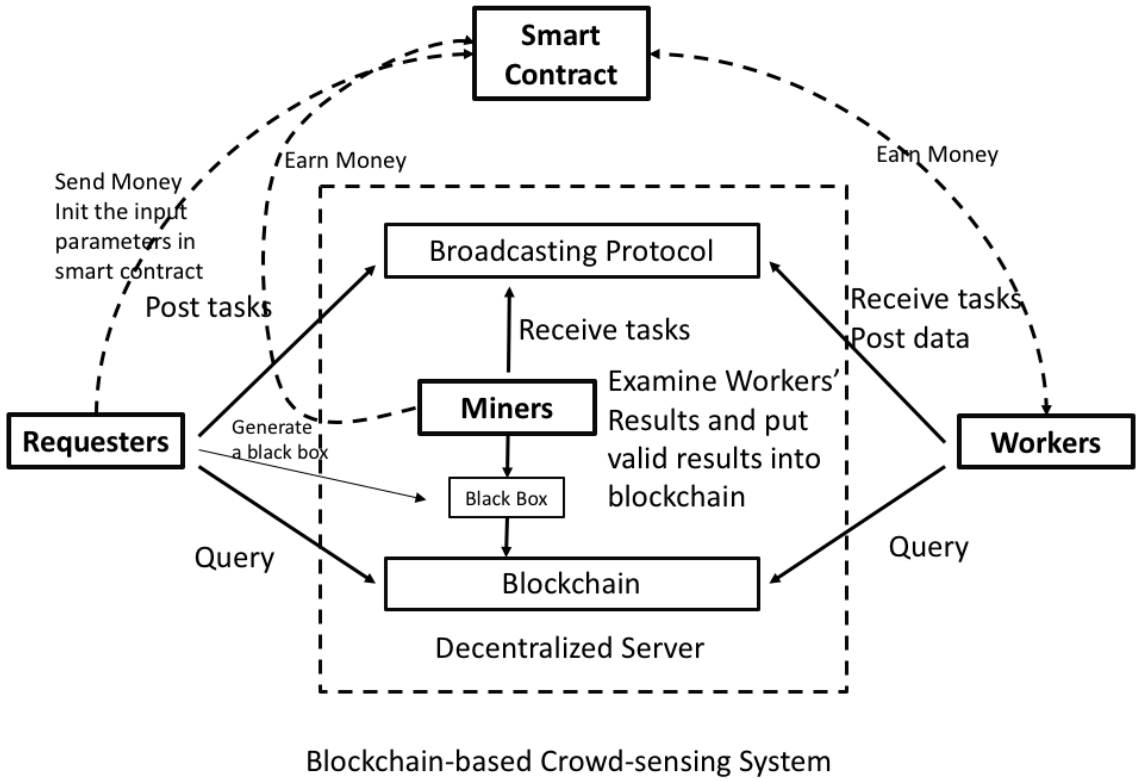

Fig 3. The introduction of bank to the blockchain-based crowd-sensing system

To illustrate, the requester enters in the system and stores a certain amount of money, e.g., bitcoins, in the smart contract protocol. After that, once workers' data are substantiated in blockchain by miners, they can get tokens to exchange money stored in the smart contract protocol. Therefore, the reputation of this system can be quickly built, and the enthusiasm of both miners and workers can be aroused as once they got works done, they can receive valuable rewards.

Also, since there are deposits in the smart contract, both workers and miners can trust the requester as a credible administrator whose reputation is authorized by his money. Therefore, the challenge of lacking trusted administrators for puzzles like protein folding and space signal searching is overcome in this proposed framework.

5. Black Box

As shown in Figure 3, requesters stipulate the examining rules by generate a black box for all of the miners, which I try to realize by the technology of Homomorphic Encryption (HE) [24-26]. HE provides methods to delegate processing of your data without giving away access to it, and Figure 4 introduces the basic operating process of HE.

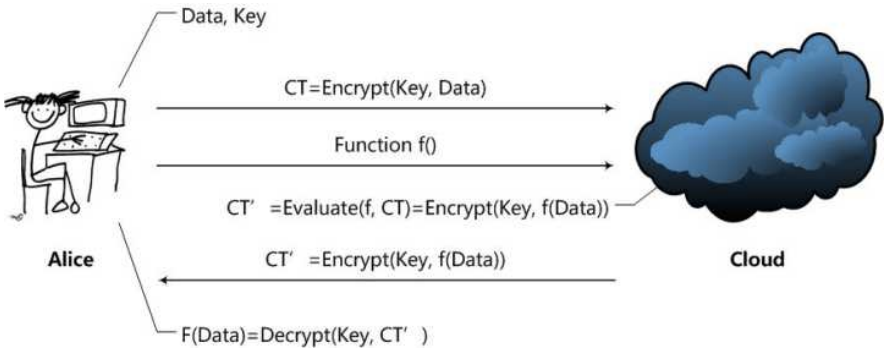

Fig 4. Brief introduction of process of HE

Actually, the black box in our framework actually is the function *F* shown in Figure 4. Requesters broadcast the black box, i.e., the function to miners, and then miners can process, i.e., examine the sensing data from workers without knowing what the data exactly looks like.

6. Design inside Blocks

This section focuses on the inside design of block structure in the proposed framework. Figure 5 helps to illustrate the structure of the block.

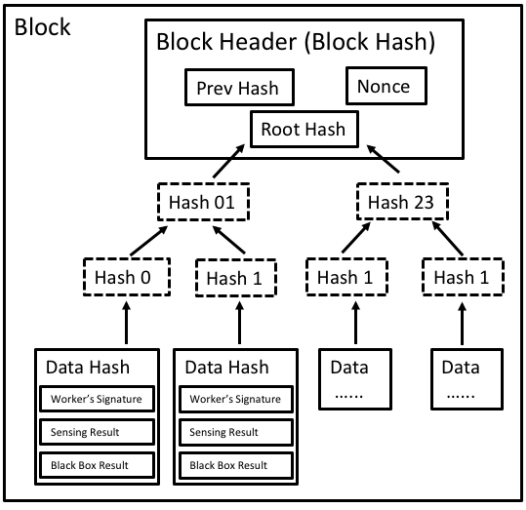

Fig 5. The structure of the block in the blockchain

As shown in Figure 5, similar with blocks in bitcoin system, the block in proposed framework also contains block header, previous block's hash, the nonce for hash puzzle and the Merkle Tree organized Data. Differently, the transaction data in bitcoin now is replaced by examined sensing-data, which are comprised of worker's signature, the sensing result and the result of black box test. What should be noticed is that the number of sensed data in the block is also fixed. Moreover, the difficulty of the hash puzzle can be self-adjusted by the framework according to the average time to find a new block.

7. Conclusion

To sum up, in this research proposal, I propose building a blockchain-based crowd-sensing system in my future study to make up for the paucity of decentralized crowd-sensing systems with reliability, security and low services fee. 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.

8. References

[1] Ma, H., Zhao, D., & Yuan, P. (2014). Opportunities in mobile crowd sensing. IEEE Communications Magazine, 52(8), 29-35.

[2] Zhang, X., Yang, Z., Sun, W., Liu, Y., Tang, S., Xing, K., & Mao, X. (2016). Incentives for mobile crowd sensing: A survey. IEEE Communications Surveys & Tutorials, 18(1), 54-67.

[3] Vergara-Laurens, I. J., Jaimes, L. G., & Labrador, M. A. (2016). Privacy-preserving mechanisms for crowdsensing: Survey and research challenges. IEEE Internet of Things Journal.

[4] Pournajaf, L., Xiong, L., Garcia-Ulloa, D. A., & Sunderam, V. (2014). A survey on privacy in mobile crowd sensing task management. Tech. Rep. TR-2014–002.

[5] Krontiris, I., Langheinrich, M., & Shilton, K. (2014). Trust and privacy in mobile experience sharing: future challenges and avenues for research. IEEE Communications Magazine, 52(8), 50-55.

[6] Cardone, G., Foschini, L., Bellavista, P., Corradi, A., Borcea, C., Talasila, M., & Curtmola, R. (2013). Fostering participaction in smart cities: a geo-social crowdsensing platform. IEEE Communications Magazine, 51(6), 112-119.

[7] Cardone, G., Cirri, A., Corradi, A., & Foschini, L. (2014). The participact mobile crowd sensing living lab: The testbed for smart cities. IEEE Communications Magazine, 52(10), 78-85.

[8] Hamm, J., Champion, A. C., Chen, G., Belkin, M., & Xuan, D. (2015, June). Crowd-ML: A privacy-preserving learning framework for a crowd of smart devices. In Distributed Computing Systems (ICDCS), 2015 IEEE 35th International Conference on (pp. 11-20). IEEE.

[9] Jayarajah, K., Balan, R. K., Radhakrishnan, M., Misra, A., & Lee, Y. (2016, June). LiveLabs: Building In-Situ Mobile Sensing & Behavioural Experimentation TestBeds. In Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services (pp. 1-15). ACM.

[10] Han, G., Liu, L., Chan, S., Yu, R., & Yang, Y. (2017). HySense: A Hybrid Mobile CrowdSensing Framework for Sensing Opportunities Compensation under Dynamic Coverage Constraint. IEEE Communications Magazine, 55(3), 93-99.

[11] Nakamoto, S. (2015). Bitcoin: A Peer-to-Peer Electronic Cash System. November 2008.

[12] Swan, M. (2015). Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".

[13] Zhang, X., Xue, G., Yu, R., Yang, D., & Tang, J. (2015). Keep your promise: Mechanism design against free-riding and false-reporting in crowdsourcing. IEEE Internet of Things Journal, 2(6), 562-572.

[14] Li, M., Lu, W., Weng, J., & Yang, A. (2017). CrowdBC: A Blockchain-based Decentralized Framework for Crowdsourcing. IACR Cryptology ePrint Archive, 2017, 444.
[15] https://en.wikipedia.org/wiki/PayPal
[16] Greenberg, A. (2016). Zcash, an untraceable bitcoin alternative, launches in alpha.
[17] Lee, C. (2011). Litecoin.
[18] http://www.gov.cn/gzdt/2013-12/05/content_2542751.htm
[19] King, S. (2013). Primecoin: Cryptocurrency with prime number proof-of-work. July 7th.
[20] https://setiathome.berkeley.edu/
[21] https://motherboard.vice.com/en_us/article/aek3za/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020
[22] Miller, A., Juels, A., Shi, E., Parno, B., & Katz, J. (2014, May). Permacoin: Repurposing bitcoin work for data preservation. In Security and Privacy (SP), 2014 IEEE Symposium on (pp. 475-490). IEEE.
[23] Dill, K. A., & MacCallum, J. L. (2012). The protein-folding problem, 50 years on. science, 338(6110), 1042-1046.
[24] Ron Rivest, Leonard Adleman, and Michael L. Dertouzos. On data banks and privacy homomorphisms. Foundations of Secure Computation, 1978.
[25] Craig Gentry. Fully homomorphic encryption using ideal lattices. STOC 2009. Also, see “A fully homomorphic encryption scheme”, PhD thesis, Stanford University, 2009.
[26] Jake Loftus, Alexander May, Nigel P. Smart, and Frederik Vercauteren. On CCA-Secure Fully Homomorphic Encryption. Cryptology ePrint Archive 2010/560.