Nat. Volatiles & Essent. Oils, 2021; 8(6): 6235-6241

NVEO
Natural Volatiles &
Essential Oils

Secure And Privacy-Preserving Crowd Sensing Using Smart Contracts: Issue And Solution

PREETHI.S[1] , Dr. E.Gajendiran[2]

[1]Assistant Professor, Department of Information Technology, Dhanalakshmi Srinivasan College of Engineering and Technology.

[2]Assistant Professor, Dhanalakshmi Srinivasan College of Engineering and Technology.

SECURE AND PRIVACY-PRESERVING CROWD SENSING USING SMART Abstract

The advent of Block chain and smart contracts is empowering many technologies and systems to automate commerce and facilitate the exchange, tracking and the provision of goods, data and services in a reliable and auditable way. Crowd sensing systems is one type of systems that have been receiving a lot of attention in the past few years. In crowd sensing systems consumer devices such as mobile phones and Internet of Things devices are used to deploy wide-scale sensor networks. We identify some of the major security and privacy issues associated with the development of crowd sensing systems based on smart contracts and Block chain. We also explore possible solutions that can address major security concerns with these systems.

Keywords Block chain ,Crowd sensing, Internet of Things (IoT),Privacy, Security, Smart contracts

1. Introduction

The high number of sensor-enabled Internet connected devices such as smart phones and Internet of Things (IoT) devices are enabling new kinds of business ventures and societal applications that are exploiting these devices not only for profit but also for the benefit of the public. As of summer of 2020, and according to recent research (as of 2021) there are around 8 billion mobile subscriptions in the world, with 5.5 billion being smart phone subscriptions . These numbers are expected to soar in upcoming years as technologies such as 5G/6G networks and more IoT devices are deployed around the world. In the past, we have seen applications of crowd sensing systems in areas such as environmental monitoring, transportation, entertainment, security, and healthcare . More recently, many countries have deployed crowd sensing systems in response to the Corona virus Disease 2019 (COVID-19) pandemic not only for epidemiology reasons (i.e., contact tracing), but also for treatment .

In addition to crowd sensing, a second set of technologies are having a tremendous impact on society. These technologies are Block chain and smart contracts. Block chain offers several services for secure data storage, retrieval, and sharing with properties such as immutability, transparency, decentralization, and fault tolerance . Smart contracts expand Block chain technology by providing means to automate transactions in a Block chain system through the specification of computer programs that encapsulate business logic and code needed to execute some actions when conditions are met . Smart

contracts enable crowd sensing to improve not only data collection and sharing in crowd sensing systems, but also to create opportunities in the development of decentralized markets wherein sensor data collectors can sell their data without the need of a centralized entity or a broker . However, this vision exposes various security issues that must be addressed. In this work, we explore these emerging issues along with possible solutions.

2. Crowd sensing and smart contracts

(i). Crowd sensing systems

The history of modern research in Wireless Sensor Networks (WSN) started with the Distributed Sensor Networks (DSN) program developed in the 1970's in the United States . This project used minicomputers and acoustic sensors to develop a system that could track low-flying aircrafts and it was considered state-of-the art during its time. The DSN project paved the way for a revolution in WSN technology and systems in the late 90's, in which networks of potentially thousands of small devices left unattended and interconnected wirelessly could monitor large areas of interest for many months, potentially years. However, actual implementations of WSNs were small-scale systems, with local and specialized focus because of deployment and maintenance costs which have made WSNs with thousands of devices impractical .During the first and second decade of the 21st century, crowd sensing systems have emerged to alleviate the deployment and maintenance costs incurred in the massive use of single WSN systems with thousands of devices by leveraging the utilization of billions of smart phones and other IoT devices owned by the general public . Use of crowd sensing systems by the general public span areas such that entertainment, transportation, environmental monitoring, among others . Recently, crowd sensing systems developed under the name of contact tracing apps have been deployed in response of the CoronaVirus Disease 19 (COVID-19) pandemic caused by the Severe Acute Respiratory Syndrome CoronaVirus 2 (SARS-CoV-2 . As these systems make use of consumer devices to conduct sensing on a large-scale, they circumvent costs associated with the deployment of networks with thousands of devices especially in urban areas presents the basic components of crowd sensing systems . Sensors: They collect data either from measurable real-world variables such temperature, heart rate, pollution, objects (i.e., photos), or Human–Computer Interaction (HCI) or system processes (i.e., how much time a person logins to a website, or opens an application). The embedding of sensors for physical quantities in portable systems is possible through the research and development of tiny machines at the micrometer scale (also known as Micro-Electro Mechanical Systems (MEMS)).

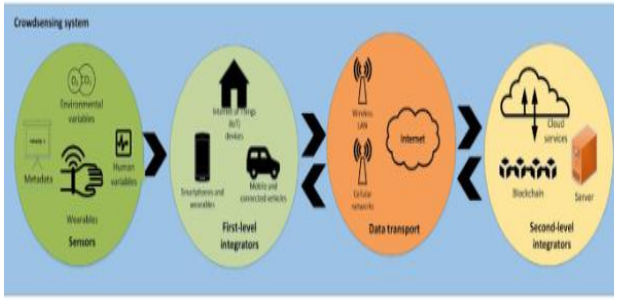

Fig. 2.1 Hardware components of crowd sensing systems

(ii). Block chain and smart contracts

Block chain is a Peer-to-Peer (P2P) technology that implements a distributed ledger and stores data in a secure, immutable, and append-only approach through consensus or agreement among the peers in a Block chain network . The structure of Block chain networks is composed of the following layers:

A P2P network: The P2P network ensures free communication among Block chain nodes. These Block chain nodes are around the globe and there is no hierarchical structure in the network. Global distributed ledger: The global distributed ledger implements the storage protocol to maintain the ledger. Each user is identified with a unique digital pseudonym (address) which is generated using public key cryptography. Communication between two addresses is carried out through a transaction. Data actions in the global ledger are conducted using a smart contract which execute the transactions. Applications: The application layer of a Block chain network implements Application Programming Interfaces (APIs) for various application scenarios.

Some of these applications may include financial services, telemetry systems, copyright protection, and digital document management platforms, among others .

the global distributed ledger consists of blocks of data chained together with cryptographic hashes. In any given block in the chain, the system stores (in all peers) transactions that are verified using a predefined set of rules to determine which transactions are valid. Only valid transactions are recorded in the Block chain. A consensus algorithm executed by all peers in the network determines the next block to be chained to the ledger and it provides strong integrity to the data stored as it allows all peers to agree on a single version of the chain (guaranteeing integrity in the chain) without a central authority. Different models for consensus algorithms have been developed with various characteristics and properties. Some examples of these models include Proof-of-Work (PoF) , Proof-of-Stake (PoS) , Proof-of-Authority (PoA) , Proof-of-Space (PoSpace) , among others .

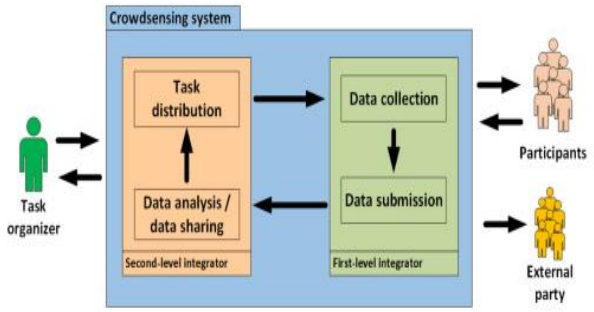

Fig. 2.2 Stages to collect and analyze data in crowd sensing systems

(iii). Enhancing crowd sensing systems with smart contracts

Smart contracts in public Block chains can enhance crowd sensing systems by creating automated agreements between task organizers and participants that guarantee not only the completion of a data collection task, but also automated payments for those types of crowd sensing systems that make use of monetary incentives for data collection. The data collected can also be directly stored in the Block chain itself, thus providing tamper-proof assurances that anyone can verify. We can classify the architectural

models for crowd sensing systems with Block chain/smart contracts support into two categories:Pure Block chain-based crowd sensing system: In this category task organizers and participants coordinate their sensing tasks through smart contracts and Block chains. Participants execute smart contracts published in the Block chain by task organizers, data collected from participants and first-level integrators is stored in the Block chain. Task organizers download data from the Block chain and participants can be paid through cryptocurrency .

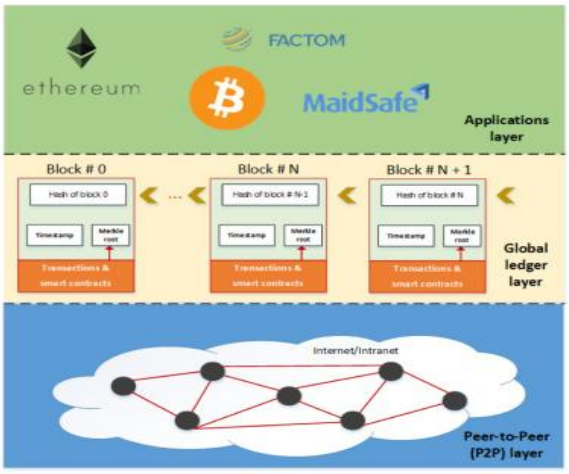

Fig.2.3 Layers in a Block chain system

Hybrid models: In these crowd sensing systems, some of the tasks (i.e., task distribution, data collection, rewards payment) are executed through smart contracts and Block chains while others are conducted using centralized crowd sensing architectures .

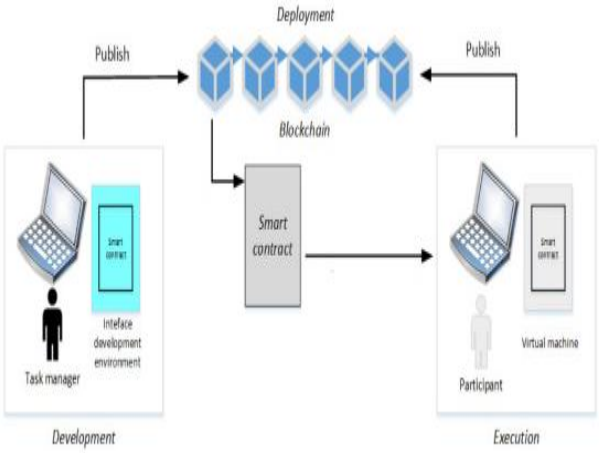

Fig. 2.4 Smart contract lifecycle

The enhancement of crowd sensing systems with smart contracts offers advantages over traditional centralized crowd sensing systems in terms of incentives, data integrity, transparency, decentralization,

fault tolerance, among others. The utilization of smart contracts and Block chain offers solutions to availability issues that are related to Distributed Denial of Service (DDoS) attacks, authentication, and privacy (i.e., anonymization of users without using third-parties because of their design).

3. Secure and privacy-preserving crowd sensing using smart contracts: Issues

Exploited bugs, errors and attacks in smart contracts have resulted in lost or stolen cryptocurrencies, some of them in the equivalent of millions of dollars . For example, the Distributed Autonomous Organization (DAO) bug exploited a recursive call in a smart contract on the Ethereum network that forced a hard fork (a change in the protocol to invalidate blocks and transactions which require an update on the nodes in the P2P network) to claim approximately 3.6 million ether (an ether being the cryptocurrency for Ethereum) . Smart contracts could be abused to instruct IoT devices to be used as zombies by botnets to attack external parties. The Distributed Denial of Service (DDoS) attack directed at Domain Name Servers (DNS) through consumer Internet-connected cameras that disrupted the Web in 2016 is an example of these type of devastating attacks . This issue is further exacerbated by the myriad of connected devices, software frameworks and service, and a lack of security by design in many of these devices' manufacturers and software/service providers. For crowd sensing systems, data integrity is affected when participants submit false or misleading data for personal profit or attack a system either unintentionally or on purpose .

According to Zhang et al. in a study wherein 20 participants collected barometric pressure data for seven days, they found that, not using a system to filter out spurious data led to a discrepancy of 20% from the ground truth. In crowd sensing systems over distributed ledgers this problem is exacerbated further because the sensing tasks is controlled by a smart contract that would pay the participants when data is submitted. Thus, participants may submit the same data under different identities to maximize profit . Privacy in Block chain systems has been receiving a lot of attention in recent years because these systems have been developed with transparency in mind. Public Block chain systems allow (as part of their design) transactions on ledgers to be publicly checked, traced, and audited to build trust in these systems. The effect is that although transactions in ledgers are registered for users under wallets and pseudonyms, they can still be potentially re-identified . In crowd sensing systems privacy is a major issue because the data collected can potentially reveal aspects considered private by the participants, making participants hesitant to participate . Privacy leaks in crowd sensing systems may hinder the participation of the crowd, and even though the design of Block chains through wallets and pseudonyms can alleviate some privacy concerns, the potential for re-identification remains an important issue.

4. Secure and privacy-preserving crowd sensing using smart contracts: Solutions

Static analysis , dynamic analysis and formal methods for malware detection have existed before the advent of general-purpose smart contracts as tools to improve security. In static analysis the goal is to analyze the source code before execution to find possible bugs in the code . A specific tool for this purpose in smart contracts is the Oyente tool . Proposed by Luu et al. this tool makes use of static analysis through symbolic expressions that represent smart contract's program variables and symbolic paths . Rules are then placed on the paths and if a path cannot satisfy a constraint, it is deemed infeasible. When a path is infeasible, the tool has found a possible bug with the program. In dynamic analysis the goal is to find bugs

and errors through the execution of fragments of code (or equivalent transformations). Some examples of this approach in smart contracts include Manticore , Methryl , VerX and KEVM . In these systems smart contracts are transformed to symbolic expressions and symbolic paths which are then executed. In the third type of techniques (formal methods), the goal is to use logic and specifications to prove program correctness. Examples of formal specifications in smart contracts include the use of the F* functional programming language , VeriSol , VeriSolid and SPIN .

As we have previously mentioned, data integrity is the problem wherein participants submit false or misleading data for personal profit, or to attack a system either unintentionally or on purpose. Solutions for this issue to improve the Quality of Information (QoI) have been proposed in the literature by using incentives and creating reputation measures for participants, having participants to submit some reimbursable deposits, and the utilization of trusted third-party verification . Solutions for participants' privacy protection in crowd sensing applications using smart contracts can be classified into three major groups: (1) Zero-Knowledge Proofs (ZKP); (2) external identity servers; (3) adaptations of k-anonymity. An example of a system that makes use of ZKP is Hawk . which keeps information about transactions encrypted in a Block chain, and the verification about the execution of a smart contract relies on zero-knowledge proofs. By making use of ZKP, the execution of a smart contract can be verified while keeping private data about the transaction, thus keeping users' identity private. In the second approach (external identity servers), systems use a registration server wherein participants register outside the Block chain to obtain public/private keys generated by a task organizer. These keys are then used to create an address which transactions use in the Block chain . In the third group, adaptations of k-anonymity (a technique for micro data release in databases have also been proposed for Block chain and crowd sensing systems using smart contracts. In these adaptations, k-anonymity has been used to create k-anonymous groups among multiple participants who trust each other , and also in frameworks wherein a single participant posts his/her collected data to the Block chain under different Block chain identifiers (i.e., addresses) .

5. Conclusion And Future Work

The dawn of Block chain, cryptocurrencies, and smart contracts in the last few years has led to the emergence of exciting applications. Crowd sensing systems is one type of applications that can benefit from the utilization of smart contracts and Block chain systems. Security and privacy are important aspects for these systems. We highlighted some of these issues along with possible solutions. Finally, we have identified future research challenges that must be addressed in the future to deploy secure and privacy-preserving crowd sensing systems that take advantage of smart contracts and Block chain technology. When smart contracts are used in crowd sensing systems, participants may be exposed to risks arising from a lack standardization in security and privacy practices in Block chain implementations.

A lack of standards can make Block chains susceptible to software bugs due to a lack of quality control in a Block chain's development process. Almost every Block chain has its own protocols, specifications, programming languages, and tools, and no standards exist to evaluate security or privacy protections in Block chain systems. Given that some of the data collected in a crowd sensing system may be human-centric data, if a EU citizen participates in a crowd sensing system supported by a Block chain, then his/her participation in the system may be against GDPR due to Block chain's immutability, transparency, and fault-tolerance features. To address this problem, one recent solution proposed the

use of smart contracts to prune a block from the Block chain if required , while some other solutions include hard-forks and redactable Block chains . The latter solution allow data to be erased without hard-forks. More research on smart contracts, digital wallets, and Block chains is needed to support crowd sensing systems to satisfy legal requirements including the right to erasure, and to support other GDPR legal requirements and future privacy laws.

References

1. Perez A.J., Zeadally S. Recent advances in wearable sensing technologies Sensors., 21 (20) (2021), p. 6828

2. Perez A.J., Zeadally S. Design and evaluation of a privacy architecture for crowd sensing applications ACM SIGAPP Appl. Comput. Rev., 18 (1) (2018), pp. 7-18

3. Park J.S., Youn T.Y., Kim H.B., Rhee K.H., Shin S.U. Smart contract-based review system for an IoT data marketplace Sensors, 18 (10) (2018), p. 3577

4. Chong C.Y., Kumar S.P. Sensor networks: evolution, opportunities, and challenges Proc. IEEE, 91 (8) (2003), pp. 1247-1256

5. Gadel-Hak M. (Ed.), The MEMS handbook, CRC Press (2001)

6. N. Vallina-Rodriguez, J. Crowcroft, ErdOS: achieving energy savings in mobile OS, in: Proceedings of the Sixth International Workshop on MobiArch, 2011, pp. 37-42.

7. M. Dong, L. Zhong, Self-constructive high-rate system energy modeling for battery-powered mobile systems, in: Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services, 2011, pp. 335-348.