future internet

MDPI

Article

Multi-Blockchain Structure for a Crowdsensing-Based Smart Parking System

Mihui Kim * and Youngmin Kim

School of Computer Engineering & Applied Mathematics, Computer System Institute, Hankyong National University/327, Jungang-ro. Anseong-si, Gyeonggi-do 17579, Korea; youngmin.hku@gmail.com

* Correspondence: mhkim@hknu.ac.kr; Tel.: +82-2-31-670-5167

Received: 21 April 2020; Accepted: 14 May 2020; Published: 16 May 2020

Abstract: As a representative example for the construction of a smart city, a smart parking system has been developed in past research and implemented through IoT and cloud technologies. However, the initial installation cost of IoT sensor devices is preventing the spread of this technology, and thus as an alternative, a crowdsensing-based system, operating through data from publicly owned mobile devices, has been proposed. In this paper, we propose a multi-blockchain structure (i.e., constructed with public chain and private chain) in a crowdsensing-based smart parking system. In this structure, many sensing data contributors participate through the opened public blockchain, to transparently provide sensing information and to claim corresponding rewards. The private blockchain provides an environment for sharing the collected information among service providers in real time and for providing parking information to users. The bridge node performs an information relay role between the two blockchains. Performance analysis and security analysis on the implemented proposed system show the feasibility of our proposed system.

Keywords: crowdsensing; multi-blockchain; interworking of public-private blockchains; smart parking system

1. Introduction

A smart city is a planned city that can collect and flexibly use data in accordance with the development of the Internet of Things (IoT) and wireless sensor network (WSN) technologies [1]. In a smart city, these advanced technologies can be applied to provide real-time information, such as up-to-date parking information, to its inhabitants. An example of such a system, which integrates IoT sensors and cloud servers in a parking system to remotely provide parking space information, has already been proposed [2]. In addition to the aforementioned use of installed IoT sensors in a smart parking system, mobile crowdsensing (MCS) technology, i.e., the method of collecting data through the cameras or sensors of mobile devices owned by the public, can also be applied [3]. MCS technology has an advantage in that the service provider can obtain large amounts of real-time data without the initial installation costs of gathering these data. In this paper, we propose a method using mobile crowdsensing technology for a smart parking system that provides parking space information.

Meanwhile, because blockchain technology that provides dispersibility, scalability, transparency, security, and safety of data management has recently been attracting attention, blockchain has also been proposed as a smart city platform [4,5]. Blockchain technology has been applied to the linking and automation of data processing for mobile crowdsensing with user compensation processing [6]. The blockchain architecture can use smart contracts to automate the provision of rewards via leveraging of the transaction records on the blockchain. These data on the blockchain can be shared transparently while integrity is maintained according to the characteristics of the blockchain. A model that utilizes a

public blockchain has also been proposed [6], but this model faces the possibility of privacy problems because the data are shared with everyone, and thus a limit to the authorized management of its functions is imposed.

In this study, we use a mobile crowdsensing service structure to build a smart parking system, and propose a multi-structure system of opened public blockchain and private blockchain with restrictions on the participating node for data management. In a public blockchain, sensing data contributors participate in providing data. In a private blockchain, service providers and data users participate in processing the collected data from the public blockchain to provide users with information about parking lots, such as locations of empty parking spaces. A bridge node joins both blockchains to connect and exchange data between the two blockchains. With such a multi-structure, the public blockchain transparently collects information from many participants, whereas the private blockchain processes and stores the information, reducing the risk of personal information exposure. Moreover, through the sharing of processing information among other service providers in the private blockchain, provision of data on the real-time parking situation, as desired by the user, can be made possible.

The contribution of this study is the design of a smart parking system, a representative application example for a smart city, with mobile crowdsensing technology and multi-blockchain structure. This structure can easily accommodate a large number of participants; collect data; provide transparency in data management; and enable service providers to lower the risk of privacy exposure and to process, share, and provide information. The proposed multi-structure and bridge node is then implemented with the representative public blockchain Ethereum [7] and the private blockchain Hyperledger Fabric [8]. Afterward, the feasibility of the proposed system is shown via experimentation with the operational performance on the implemented system, and the safety pursued by the proposed system is revealed via security analysis.

The structure of this paper is as follows: Section 2 introduces the basic techniques for mobile crowdsensing and blockchain, and Section 3 describes the structure and function of the system proposed in this paper. Section 4 describes the implementation of the proposed system, and Section 5 analyzes the performance results and evaluates our system in terms of security. Finally, Section 6 presents the conclusion of this study.

2. Literature Review

This section introduces mobile crowdsensing, blockchain technology and its structure, and multi-blockchain, through related researches.

2.1. Mobile Crowdsensing

Mobile crowdsensing (MCS) technology is a paradigm that has emerged with the development of mobile devices and mobile communication technologies, such as smartphones and cars, with high processing speeds and multiple sensors. As shown in Figure 1, MCS technology has a structure wherein the service provider collects and processes the sensing data generated by using the sensing, computing, and communication functions of the corresponding devices of a crowd, and provides a new service to users based on these data and functionalities. The characteristics of MCS, compared to those of traditional wireless sensor networks, have been presented in past literature [9]. Among these, we introduce four MCS characteristics related to the system proposed in this paper.

Figure 1. Structure of the crowdsensing system.

First, MCS does not require the building of sensors, which are the foundation for providing information services in new places. Unlike the WSN model, which requires an underlying infrastructure, a proposed system that uses MCS will have more data contributors as the number of users in the service area increases. This is because data users can act as data contributors. This is an easy way of collecting data in crowded areas but can be a disadvantage in areas with few users. However, inducing contributions via coordination of incentive models can minimize the shading of areas in data collection.

Secondly, leveraging existing devices can reduce infrastructure investment costs. Similarly, a network for providing a service may use a communication network of smartphones or mobile devices already used by users. This means that the service coverage can be broadly set up without the building of a new network.

Third, MCS utilizes smartphones and mobile devices that users use directly. The users' involvement in delivering the data allows them to collect the data they need without complex algorithms or the addition of many sensors. MCS systems that work with incentive models can motivate users to validate the data directly.

Finally, the need for sensor maintenance reduces. Contributors take the necessary steps to use their devices even when these devices encounter a problem, such as a short interruption in the network of contributors who wish to provide data. In other words, even when a malfunction occurs, the contributors can wait to deliver the data that they want to contribute to the service provider after solving the problem by themselves.

2.2. Blockchain and Its Structure

Satoshi Nakamoto first proposed blockchain in 2008 in his paper in Bitcoin [10], an electronic money system. The consensus algorithm maintains the integrity of transactions and data in such a way that multiple nodes have the same bitcoin ledger, which separates accounts based on public keys. Since Bitcoin, smart contracts have emerged for the publishing and execution of automation contracts on the blockchain and for the trade-in of money [11]. A smart contract is a function that executes the contents of a transaction automatically when the contract conditions are met. The execution results of smart contracts are recorded in blocks that cannot be modified or deleted in the repository.

If the crowdsensing system applies blockchain technology, incentives can be provided to users who participate in sensing based on transactions, except in the case of preventing malicious users from providing fake data for compensation. Based on a method suggested in past literature [12], the usefulness of the information can then be judged, and the compensation can be decided.

The consensus algorithm determines how to define block creators to have the same shared ledgers among participants and to create a block with these block creators. According to this consensus algorithm, blockchain types are divided into the public blockchain and the private blockchain [5]. In a public blockchain, any node can participate in the consensus process of blockchain and create a block [13]. Since any user can participate in the blockchain, several techniques are applied to prevent malicious users from creating blocks for malicious purposes. A private blockchain, meanwhile, is a way of restricting which nodes participate, and thus the transaction speed is fast. The private blockchain has fault tolerance, but has a few Byzantine tolerance properties because of the precondition that only trusted nodes can participate [13].

A comparison between public and private blockchains is made as follows [5]: In the case of public blockchains, anyone can participate in the consensus process, and data tampering is almost impossible. At the same time, it is difficult to establish access control to data or consensus processes. Meanwhile, in the case of a private blockchain, the read permission of the block or participant in the consensus process can also be controlled. However, if the private blockchain accepts a large number of unspecified untrusted participants, it can cause the data on the blockchain to become unreliable. The transaction speed is faster than that of the public blockchain because the consensus algorithm is simplified. Public blockchain can be used for mobile crowdsensing that requires public participation

and a public verification process, whereas a private blockchain can provide a service with minimum personal information exposure to users via formation of a blockchain between trusted service providers.

2.3. Multi-Blockchain and Privacy-Preservation

The popular Bitcoin is based on a public blockchain structure for the whole world. It can be used around the world in a system that is not specific to a particular region, but it can take a long time for a deal to be made. Although several blockchains, such as Ethereum, have tried various improvements, such as consensus algorithm optimization, to provide transaction speeds suitable for sensor networks with smart contracts, the transaction speed improvement of public blockchains is currently insufficient [13].

To overcome the limitations of blockchain services targeting the world, studies to develop blockchains with locality and to exchange information among various blockchains have been conducted [14]. In other words, to utilize the multi-blockchain, a communication scheme between two blockchains has been created, demonstrating the possibility of connecting several blockchains using protocol design [15]. A system that connects several blockchains with the routers of blockchain has also been proposed [16].

The hottest research topics in MCS are the privacy preservation of a contributor to participate in MCS without worrying about privacy exposure and the incentive mechanism encouraging a lot of participation. In general, sharing the sensing data (e.g., identity, location, and life pattern) causes a privacy exposure problem, and thus the tradeoff problem between incentive payment and privacy preservation exists. Various mechanisms [a1-a4] to resolve the tradeoff problem have been proposed. The problem of location protection issue for task allocation (i.e., a process to recruit workers and assign them with sensing tasks) under untrusted server has been dealt with [17]. The personalized location protection has been designed, considering different protection demands of workers. A location aggregation method clustered users into groups for k-anonymity preserving, mitigating the incurred information loss [18]. An incentivizing data aggregation mechanism with privacy preservation has been proposed, incorporating workers' reliability and privacy costs and integrating data aggregation and data perturbation mechanisms [19,20]. However, collaborating *K*-nodes for anonymity are required for data aggregation and perturbation, and may cause privacy problems if adversarial cooperative nodes exist.

In this paper, we design a bridge node for 1:1 connection and information exchange between two blockchains. In a multi-blockchain, we utilize the advantage of connecting public blockchain and private blockchain; i.e., automating the incentive model through a public blockchain suitable for mobile crowdsensing, and delivering the sensitive information or difficult-to-contain information in a block on a private blockchain as a medium. Moreover, the private blockchain provides an environment for sharing the collected information among service providers in real time and for providing parking information to users. That is, the proposed structure includes a process for the secure delivery of sensing data, a transparent incentive payment process, and a process for sufficient information provision through sharing information by service providers. When data, such as photographs, are collected through public-blockchain-based mobile crowdsensing, the vehicle number or the face of a person may be directly exposed. To protect the privacy of the sensing information, the contributor receives the secure session information through the blockchain and directly delivers it to the service provider. Moreover, because the blockchain is unsuitable for delivering unstructured data, such as photos, we design for the contributor to deliver the data to the service provider. If the mobile device of contributor can preprocess the data, i.e., removal of sensitive information and transformation to structured data, a method that has been previously proposed [21,22] can be applied to resist the passive attack from honest-but-curious service providers and to enhance the efficiency of data transmission.

3. Proposed System

In this section, we propose a structure that combines multi-blockchain with mobile crowdsensing for the development of a smart parking system.

3.1. Overview of Proposed System

The proposed scheme uses two types of blockchain. One is a public blockchain, wherein contributors participate in MCS, and the other is a private blockchain, wherein service providers and users participate in the processing, provision, and use of data. Bridge nodes participate in both blockchains to transfer data between the two blockchains.

Figure 2 shows the overall schematic structure of the system proposed in this paper. Arrows indicate the direction of the process of data exchange between the objects. ① is a public blockchain, in which the session management for data provision module and the incentive management module operate, and ② is a private blockchain, in which the session management for data gathering and the data processing module operate.

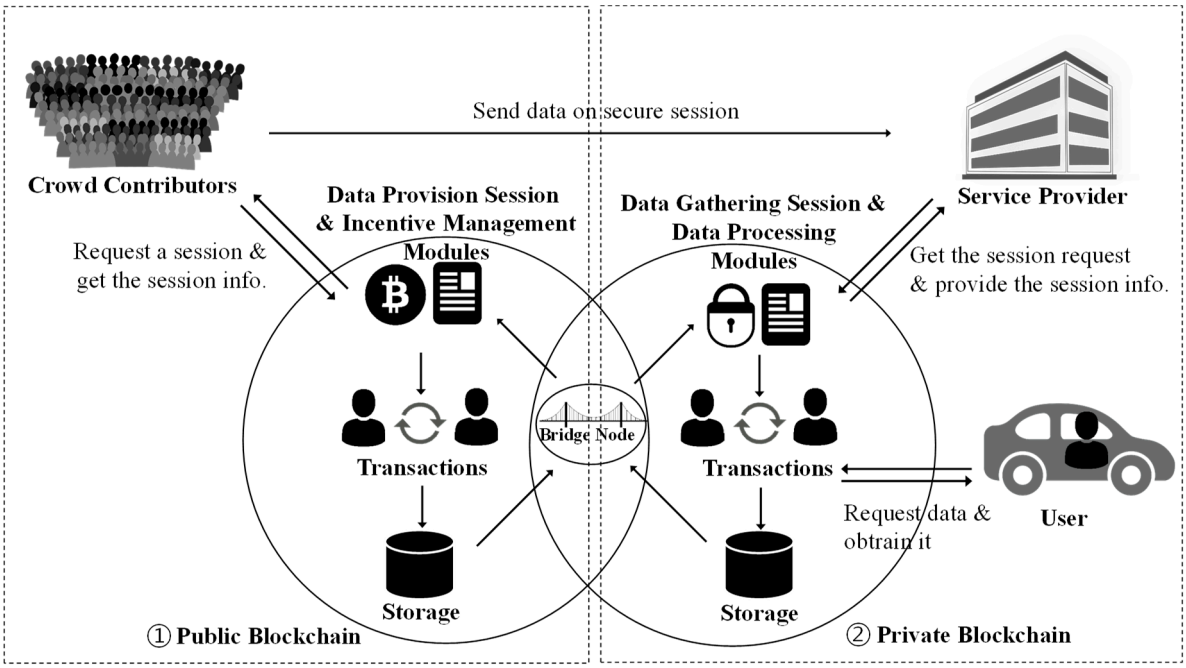

Figure 2. Structure of the proposed system.

Crowd contributors provide data to service providers using smart contracts placed on the blockchains. The transaction is executed through the deployed smart contract, and the result is stored in a public block. The bridge node executes the corresponding contract in the private blockchain based on the block contents of the public blockchain and stores it in the private block.

The service provider processes the data delivered by the contributor, for the service user to be able to identify the parking space. When the user confirms the data delivered by the contributor, verifies its validity, and distributes it to the private blockchain network, the bridge node executes a contract for reward payment to the public blockchain and stores it in the public block.

The service provider checks the validity of the data delivered by the contributor, stores it on local storage, provides it also to the private blockchain, and provides the corresponding parking space information when requested by the service user. The user checks and uses the validity of the provided parking space information, and when the validity information is announced to the private blockchain network, the bridge node executes a contract disclosing incentive information for reward payment in the public blockchain and stores the incentive information in the public block.

When a user searches through a distributed application (dApp) for a parking lot at a location that the user wants to use, the user finds the service provider of the parking lot searched through a smart contract of the private blockchain, and the smart contract sends a data request to the service provider of the corresponding parking lot. The service provider finds the requested data to provide and record the log information for the provided data in the private blockchain, and provides the data with the data hash to the user.

A bridge node is one or more nodes connected simultaneously to a public blockchain and a private blockchain. The bridge node monitors both blockchains, and when confirming a transaction to be performed in one blockchain, it transmits the relative information of the transaction to the other blockchain based on the contents of the transaction. What should be checked on both blockchains are the processes of establishing a session to transmit data, and of paying the reward for crowdsensing.

3.2. Public Blockchain-Based Data Provision Session and Incentive Management

Figure 3 is a structural diagram of the proposed system, showing the functional modules and data flow of each entity with which the contributors, service providers, and users interact, and the bridge nodes through which the two blockchains communicate. The functions in the module of each blockchain can be implemented as smart contracts, and the functions of the bridge node can be implemented as a process. The overall processes of the proposed system consist of the following: the data provision process (1.1.1–1.3.2), data acquisition process (2.1.1–2.2.2), and reward payment process (3.1.1–3.2.2).

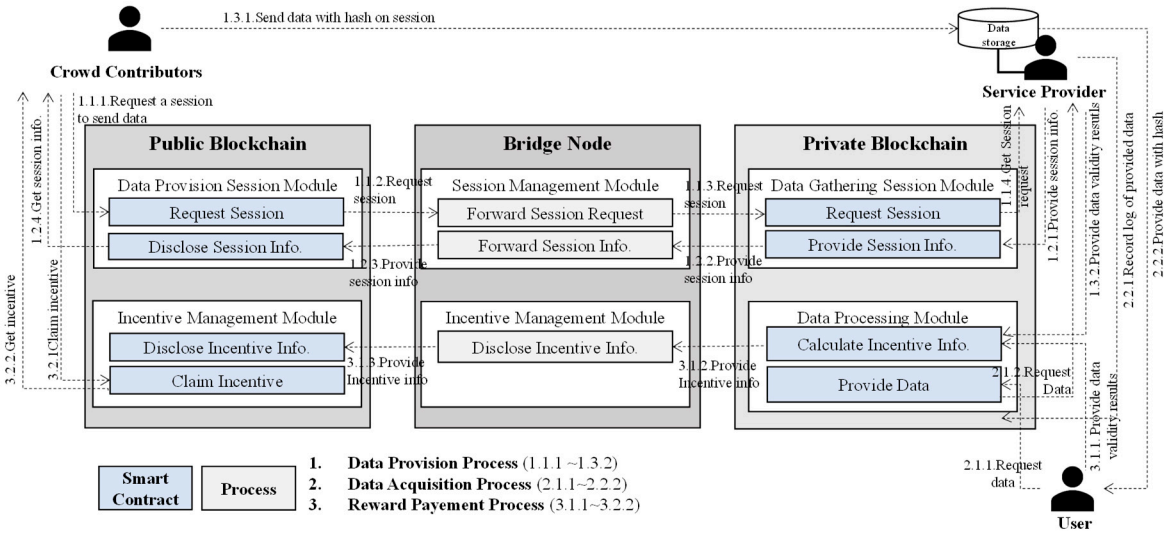

Figure 3. Functional modules and data flow of the proposed system.

The public blockchain consists of a data provision session module and an incentive management module. The data provision session module requests a session through a bridge node to a service provider operating in the private blockchain network, according to the request from the contributor. The data provision session module then provides the received session information to the contributor. The incentive management module discloses the incentive information on the block of public blockchains, for the contributors to obtain when claiming the incentive.

The bridge node consists of a session management module and an incentive management module. The former exchanges the request of session information and the created session information between the public blockchain and the private blockchain, and the latter delivers the reward information.

The private blockchain consists of a data gathering session module and a data processing module. The data gathering session module manages the session information created by the service provider, based on the session request transmitted through the bridge node. The data processing module

calculates the effectiveness and reward amount of the contributor's data and provides the calculated incentive information. Based on the data request of a user, the data processing module searches for the service provider that can provide the requested data, and then forwards the request to that service provider.

The following describes each blockchain in more detail. As shown in Figure 4, in the public blockchain, a contributor participates in crowdsensing, and a bridge node is involved. In this blockchain, smart contracts are used to obtain session information, to deliver data from contributors (i.e., named Request Session and Disclose Session Info.), and to claim and pay incentives (i.e., named Disclose Incentive Info. and Claim Incentive). The purpose of the public blockchain is to incentivize and encourage many contributors, through mobile crowdsensing, to collect the latest data. The bridge node plays a role in providing data from the public blockchain tailored to the purpose of the private blockchain.

Incentive storage (i.e., blockchain) has the information about the provided data and corresponding incentives. The information consists of the contributor (i.e., ID and public key), service provider (SP) in the private blockchain to which the contributor transmits the data, transaction ID used in the session request, session information encrypted with the public key of the contributor, use of contributed data, and disclosed incentive information. The contributor can decrypt the session information with its own private key to establish the data session with the service provider. During the performance of the data provision process, contribution information, SP ID, and transaction ID for session request are stored. Moreover, the use of contributing data and incentive information are stored for the reward payment process, and these pieces of information are mapped with the transaction ID of the session request.

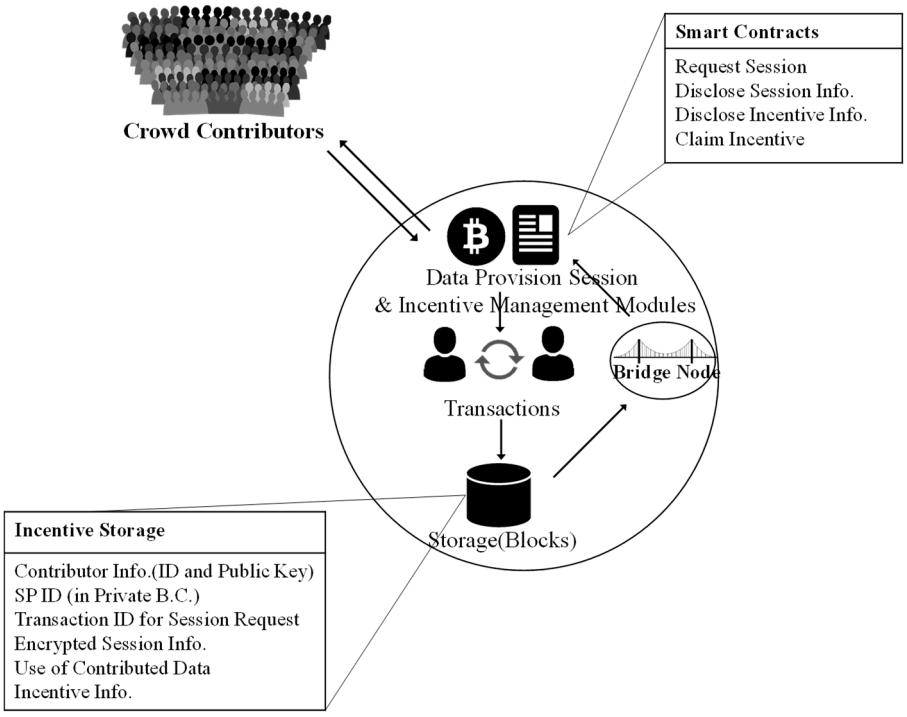

Figure 4. Structural diagram of a public blockchain.

Contributors provide data (e.g., a picture of a parking lot) for mobile crowdsensing on the public blockchain. The contributors provide the data to the service provider, and in exchange, receive compensation.

The service provider should gather data from contributors to provide parking information (e.g., parking availability or the number of empty parking spaces) to the user. Therefore, the contributor leaves a transaction requesting a data session with the service provider, with the ID of the service provider and his ID and public key, to directly transmit the data (e.g., parking information or photograph) to

the service provider. When this transaction is stored in the block, the bridge node transfers the data to the private blockchain. After obtaining the session information that is encrypted and returned with the public key of contributor, the contributor establishes a session with the service provider and transmits the data through the session. Subsequently, the contributor can be compensated, according to the verification result of the data evaluated by the user, and the use of the contributing data.

3.3. Private Blockchain-Based Data Gathering Session Management and Data Processing

As shown in Figure 5, the private blockchain consists of service providers, service users, bridge nodes, and smart contracts for session management and data processing. The purpose of a private blockchain is to support the service provider in gathering the data from contributors and to deliver information to the users who request for it; a private blockchain records the data delivered from the contributors to the users who need the data, and leaves a record to reward the contributors who provided the data.

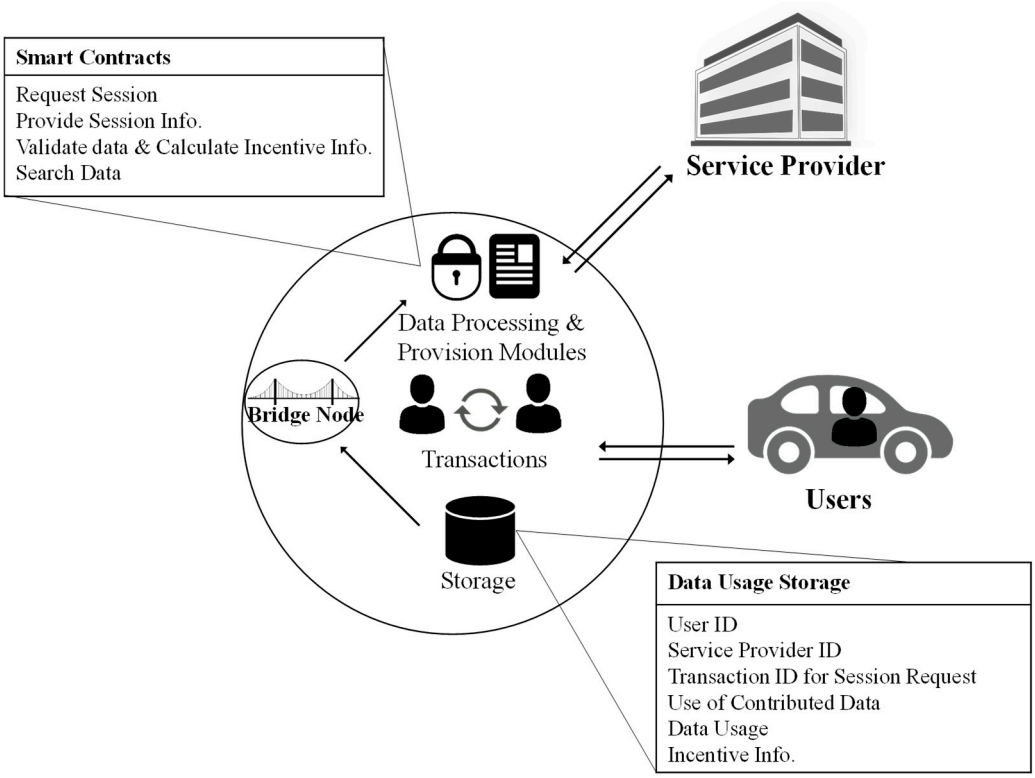

Figure 5. Structural diagram of a private blockchain.

A service provider is an entity that owns or manages a parking lot. The service provider, participating in the private blockchain, creates a session to receive data (e.g., photos of parking lot) when a session is requested; encrypts the session key with the public key of the contributor included in the transaction; and returns session access information, encrypted session key, and recipient information (i.e., contributor) together in a transaction. Afterward, the service provider receives parking information through a created session, and records calculated reward information in the private blockchain according to the validity of the data and the user's usage of the data. In addition, when receiving parking data (e.g., photograph), the service provider should process personal information identifiable from the data, to prevent this personal information from being identified, and store only the parking information (e.g., time and number of free parking spaces) required by the user.

A user is an entity who actually uses the data refined by the service providers. The user requests for information about a parking lot within a certain distance and leaves a transaction to pay a certain amount of reward to a contributor who provides the data on the parking lot that the user actually

selects. The private blockchain includes smart contracts related to session management and data processing named Request Session, Provider Session Information, Calculated Incentive Information, and Search Data.

Data usage storage, (i.e., blockchain) which consists of information about data usage stored in the blockchain, is stored via the following process. When the service provider confirms the session request received through the bridge node, it collects the contributor ID of the public blockchain and the public key of the contributor for a response. Afterward, the session information is encrypted using the collected public key, and the session information is disclosed to the public blockchain.

The user uses the smart contract (named Search Data) to request the necessary data from the service provider and leave the record on the private blockchain (i.e., User ID and Service Provider ID). The transaction includes the location information of the user, to determine which contributor's data are used. To pay compensation for the data, the contents to be disclosed on the public blockchain are first recorded on the private blockchain based on the use of the contributed data. The calculated incentive information is also recorded on the private blockchain.

3.4. Advantage of Multi-Blockchain Structure

Blockchain can prevent the deletion of data and maintain its integrity. However, in the case of a public blockchain, its disadvantage is that setting authority for access to information, for when a service is being designed, is difficult because of the feature that all users must share the ledger. When the aforementioned service is applied to one blockchain, there is a risk that a data-request transaction by a user in need of parking service is exposed as it is.

We design multiple blockchains (i.e., public and private blockchains) to overcome the risk. In the case of a public blockchain, all nodes share the same blocks. In the open environment of the public blockchain, all transaction records are publicly accessible, providing transparency, scalability, and stability, and anyone is allowed to participate. In the case of a private blockchain, however, only the necessary blocks can be shared for each node for each purpose, allowing services to be provided without exposure of personal information. Our system can use both blockchains organically via maintenance of anonymity, application of incentive models on public blockchain, and provision of data processing and services on the private blockchain. Moreover, the bridge nodes participate in both blockchains to provide smooth linkage and transfer data between the two blockchains. The bridge nodes monitor both blockchains, and execute the corresponding contract in the private blockchain based on the block contents of the public blockchain and vice versa.

When the two blockchains are divided according to their respective purposes, minimizing the exposure of personally identifiable information, which is an important requirement of mobile crowdsensing, is made possible, and the advantages of both blockchains that are suitable for crowdsensing are obtained. To identify individuals and provide appropriate services, a private blockchain is constructed and grafted in such a way that it could be viewed only by entities that need the data.

When data, such as photographs, are collected through mobile crowdsensing, the vehicle number or the face of a person may be directly exposed, thereby causing a privacy violation via identification of the individual. In addition, if data collection and processing are performed in a public blockchain, a user may be identified through pattern analysis of the location or of the data-providing cycle where the data is provided. The multi-blockchain can therefore be used to protect the user via processing and storage of personal information through a private blockchain, instead of through a public blockchain, to reduce the risk of exposure. Moreover, the risk can be reduced further through preprocessing of personal information in the device of the information provider, using a method that has been previously proposed [21,22].

4. Implementation of Proposed System

4.1. Implementation Environment

This section describes the details for implementing the proposed system. To construct the proposed multi-blockchain network, we implement a public blockchain, in which contributors and bridge nodes participate via Ethereum [7], and a private blockchain, in which service providers, bridge nodes, and users who utilize data, participate via Hyperledger Fabric [8]. The experiment for measuring transaction execution speed uses the Ropsten test network [23] to test the Ethereum environment.

Table 1 shows the version of the platform used to build the blockchains and the hardware specifications of the experiment device. We participate in Ethereum as an Ethereum test network node with Geth [7]. All transaction gas is set to the average of gas prices for the entire Ropsten network.

Table 1. Development environment.

Platform and Machine	Version and Specification
Ubuntu [24]	18.04.3 LTS
Geth(Go-Ethereum) [7]	1.9.9-stable-01744997
Hyperledger Fabric [8]	1.4.3
Development machine	CPU: AMD Ryzen 5 1600 RAM: 4096 MB Storage: 500 GB NVMe SSD

A bridge node running via participation in both Ethereum and Hyperledger Fabric is responsible for detecting specific transaction events and exchanging data between the two blockchains. For communication between the contributor in the public blockchain, and the service provider and the user in the private blockchain, the bridge node delivers necessary data at the requests of the contributor, user, and service provider. Methods are described according to each of the parts for the contributor, user, and service provider.

4.2. Process for Contributor

A contributor must deliver unstructured data, e.g., photographs, to provide data for the mobile crowdsensing. Because the photo may include information outside the intended purpose (e.g., a vehicle number and a person), information that can be identified in the photo should be removed as much as possible in the contributor device [21,22]. The service provider must perform the task of extracting parking saturation information based on the data provided by the contributor. To do this, the data of the contributor must be delivered to the service provider; however, the blockchain is unsuitable for delivering unstructured data, such as photos.

Therefore, a contributor requests a session for directly delivering unstructured data to a service provider through a smart contract, as shown in Figure 6. The “Confirm tx” in the sequence diagrams refers to the transaction confirmation, whereas “[PK]information” and “[SK]information” denote the information encrypted with the public key and the session key, respectively. The contributor transmits the information of the service provider and his own public key together through the session request contract of the public blockchain. When the content is confirmed in the public blockchain, the bridge node delivers the content to the private blockchain. When the delivered transaction is approved again, the service provider creates a session, encrypts a session key and the session information with the public key received with the identification information of the contributor, and sends it back to the blockchain. The contributor decrypts the session information, with which the photo would be delivered through the encrypted session information, and directly transmits the data through the session.

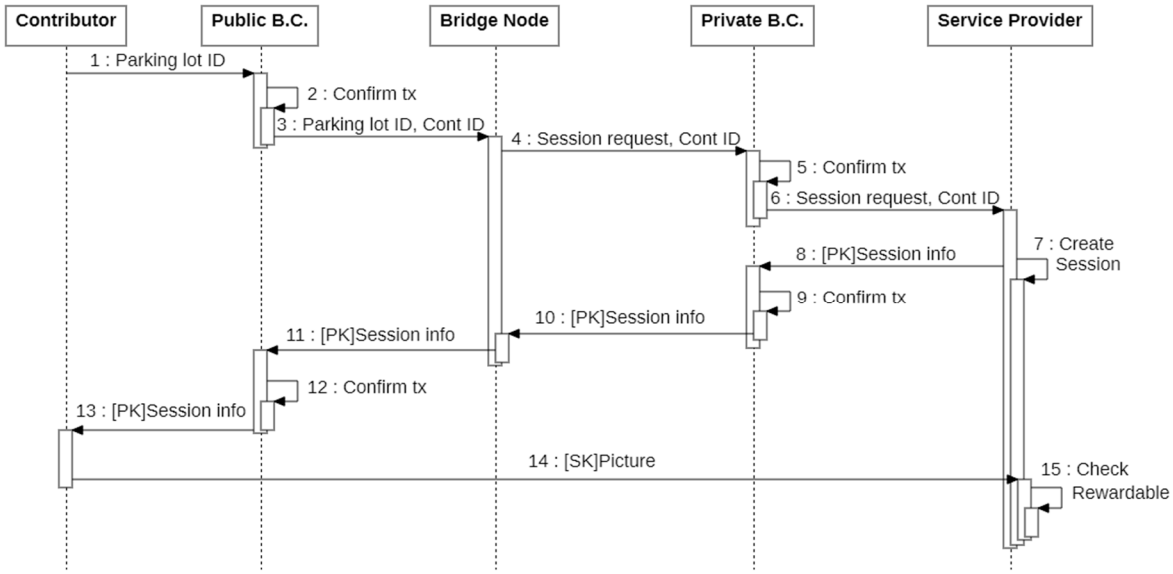

Figure 6. Sequence diagram for data contribution.

The service provider who receives the photo from the contributor determines whether the photo actually helps other users (e.g., checking the photo if it matches the location, or checking the hash code for the received information). The result of the validity judgment of the picture is stored in a transaction, to allow the reward to be delivered to the contributor, as shown in Figure 7. The service provider performs a transaction on the private blockchain that indicates that the contributor can receive the reward, without directly exposing the reward information of the specific contributor to the public blockchain, through the smart contract (i.e., encrypting the information in the transaction with the public key of the contributor that provided the data). The bridge node executes the "Disclose Incentive Information" contract in the public blockchain (i.e., changing its contents to a request to transmit actual cryptocurrency to the public blockchain) and thus leaves the incentive information in a block. Afterward, the contributor claims the reward and obtains the actual cryptocurrency.

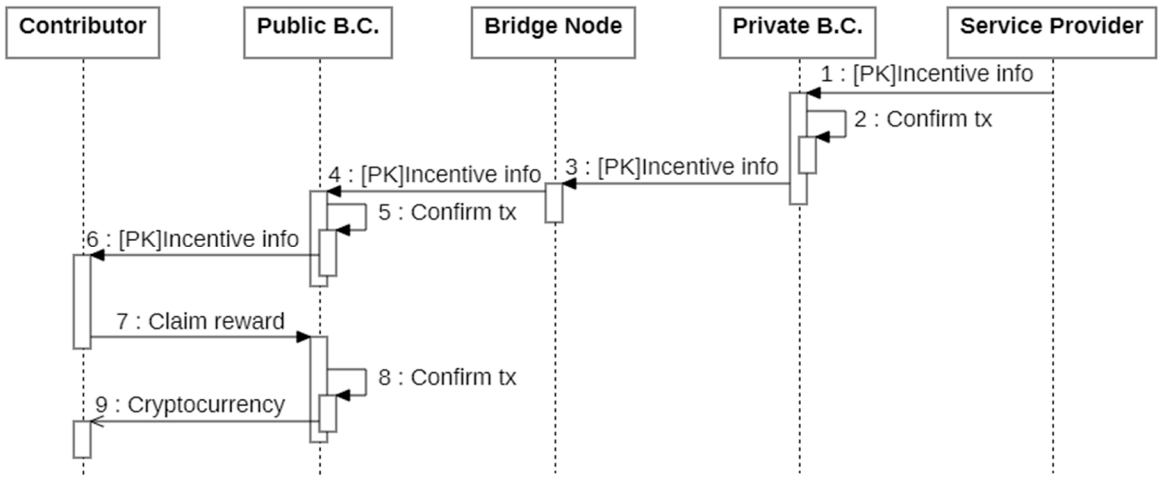

Figure 7. Sequence diagram for the reward.

4.3. Processes for Service Provider and User

When the service provider receives the parking lot data (e.g., photos), it calculates and estimates the congestion level of the parking lot, using methods developed in past research [22]. Subsequently, if requested by the user, parking lot information is provided via transmission of the congestion degree

of the parking lot to the user. The validity of the information is determined according to the inquiry and evaluation of the user, and the degree of compensation to the contributors for this information is calculated.

Users belong to the private blockchain and can request data. The requested data are directly acquired from the service provider, as shown in Figure 8.

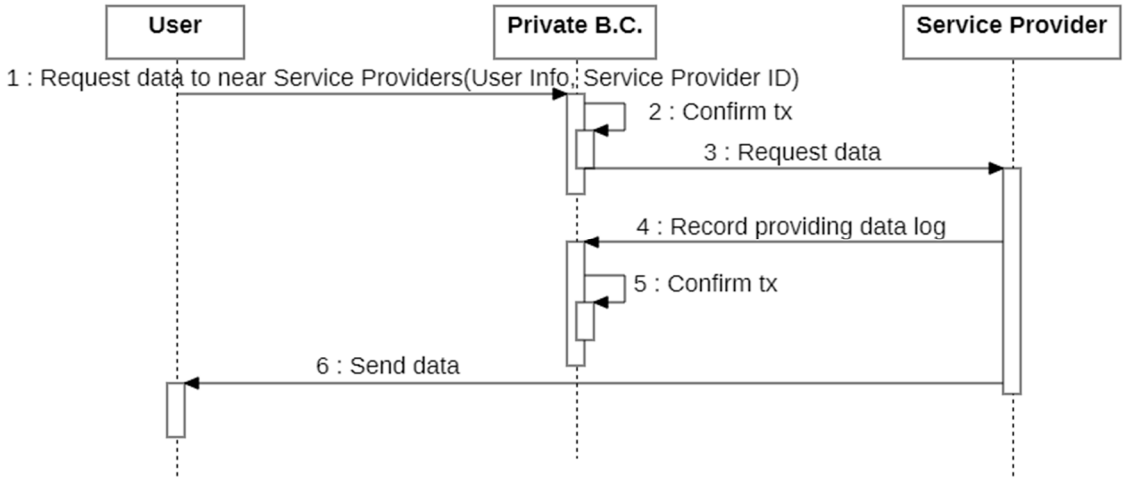

Figure 8. Sequence diagram for the data request of a user.

5. Performance Evaluation

In this section, we implement the proposed system and analyze its performance through experiments. First, we measure and analyze the execution times of the main functions on the contributor and user sides of the proposed system using the multi-blockchain. In addition, to analyze the overhead of the multi-blockchain structure, we compare our system with the case wherein it is implemented as a single blockchain. Second, we consider the congestion situation of the service when the proposed system is applied to the actual operating blockchains. Third, we analyze our mechanism in terms of security.

5.1. Experimental Analysis

First, we measure the execution time on the contributor side of the proposed system. Figure 9 is a time measurement of the contributor's data contribution processing illustrated in Figure 6 (numbers 1–10), where the session information is disclosed at the public blockchain after the contributor requests a session to provide the data. That is, the measurement starts from when a request is made to the Ethereum, through the calling of the command from the contributor, and the transaction can be confirmed in the Ethereum block. The bridge node then finds the transaction and delivers it to the Hyperledger Fabric. We measure the time until the session information generated by the service provider is disclosed to the bridge node through the Hyperledger Fabric. The graph shows the results of 100 executions, and the difference in execution time can be seen in each execution. To analyze the factor that has the greatest influence on the execution time, the experiment is divided into parts (i.e., Ethereum part and Hyperledger Fabric part).

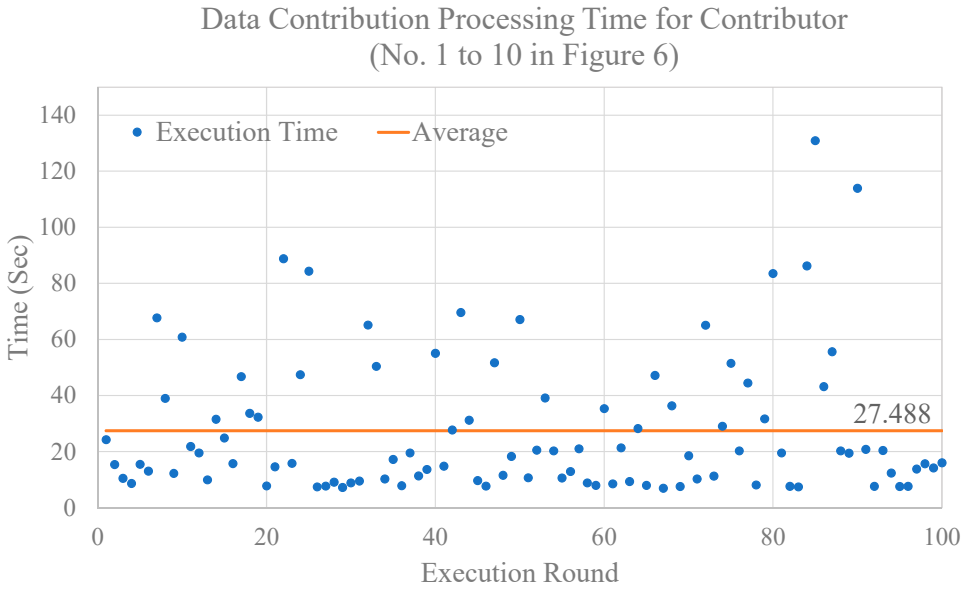

Figure 9. Data contribution processing time in each round for the contributor.

Figures 10 and 11 show the execution time portions for data contribution processing for each execution in Ethereum (1–3 in Figure 6) and Hyperledger Fabric (4–10 in Figure 6), respectively. These time portions are measured when the process has been divided into the Ethereum and Hyperledger Fabric parts. The average and standard deviation for the Hyperledger Fabric data in Figure 11 are approximately 3.7896 and 0.197, respectively, whereas the average and standard deviation of the execution time in the Ethereum portion, shown in Figure 10, are 23.698 and 24.757, respectively. Through this experiment, most of the execution time of the blockchain-based application was observed to be highly dependent on the transaction speed of the public blockchain Ethereum; i.e., fluctuating and time consuming. When these results are analyzed, they can be found to reflect a case where block creation consumed a large amount of time while being pushed from the priority of other transactions in the Ethereum test network. Unlike in the test network, if the transaction is performed on the main network of Ethereum, the block creation time will be about 15 s [25], resulting in uniform results. Moreover, if another blockchain with a faster block creation time (e.g., ripple, with as little as 3.5 s [26]) were to be used for the public blockchain part of the proposed system, the execution time could be reduced.

Figure 12 shows the amount of time for the user to request 10 instances of data and receive them (numbers 1–6 in Figure 7). The graph shows that the standard deviation is small and that it takes the quantitative time. That is, it is possible to confirm a fast and stable execution in the Hyperledger Fabric for the data acquisition of the user.

As the second experiment, to analyze the overhead of the proposed system with the multi-blockchain structure, we compare the proposed system with a system operating on a single blockchain. To do this, as shown in Figure 13, two structural block data structures are constructed, and the execution speeds of the contracts operating in each data structure are measured. Ethereum test network Ropsten is used for the single blockchain, whereas the multi-blockchain test network is the same as in the first experiment (i.e., Ethereum test network Ropsten and Hyperledger Fabric).

Figure 14 refers to the block data structure specified in Figure 13, and shows the difference in the transaction confirmation times between the proposed model and the single blockchain model in the public blockchain. In the Ethereum Ropsten test network, a delay phenomenon, in which the transaction execution times of less than about 5% of the total experimental results exceeded 2 min, occurred because of transaction delays. Because the results are difficult to see in terms of a general situation, we compare the experimental results by removing the outliers (i.e., top 5% of the execution times). In these modified results, the proposed system does not have a significant difference in terms of

execution time, except in the time it takes to transfer data to another blockchain (i.e., private blockchain). Meanwhile, for data that require access control, the multi-blockchain structure is advantageous in that the data can be managed in separate blockchains.

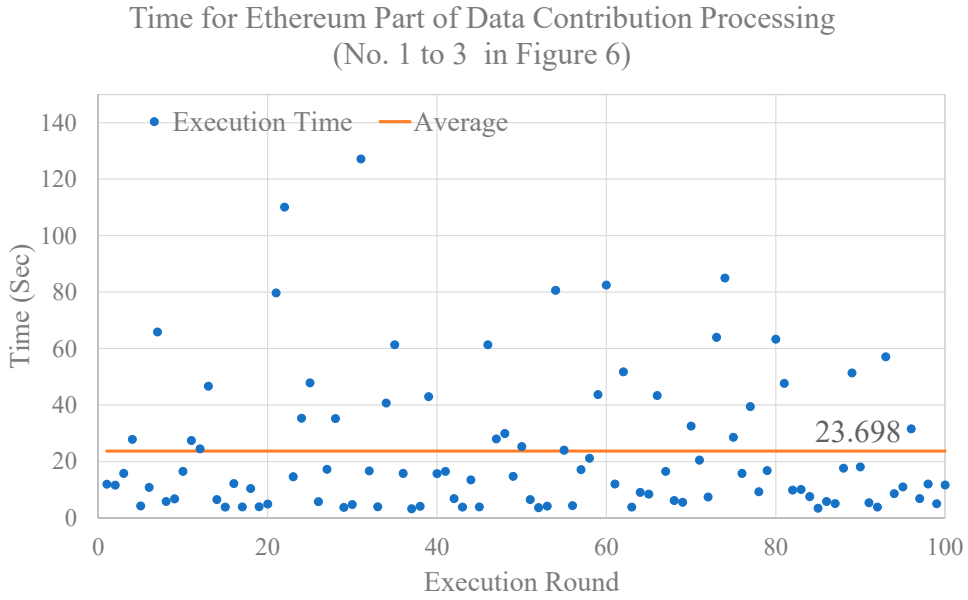

Figure 10. Data contribution processing time in each round for the Ethereum part.

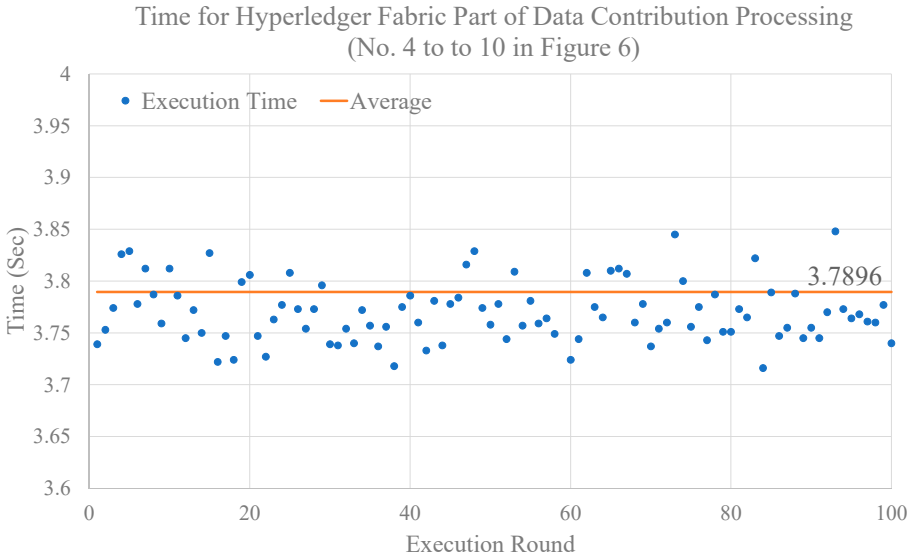

Figure 11. Data contribution processing time in each round for the Hyperledger Fabric part.

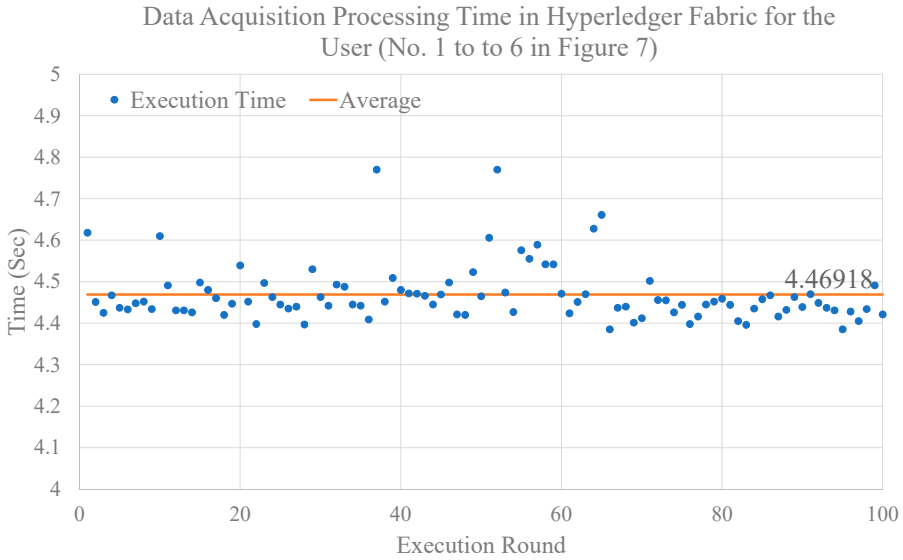

Figure 12. Data-obtaining time in each round for the Hyperledger Fabric part, for the user.

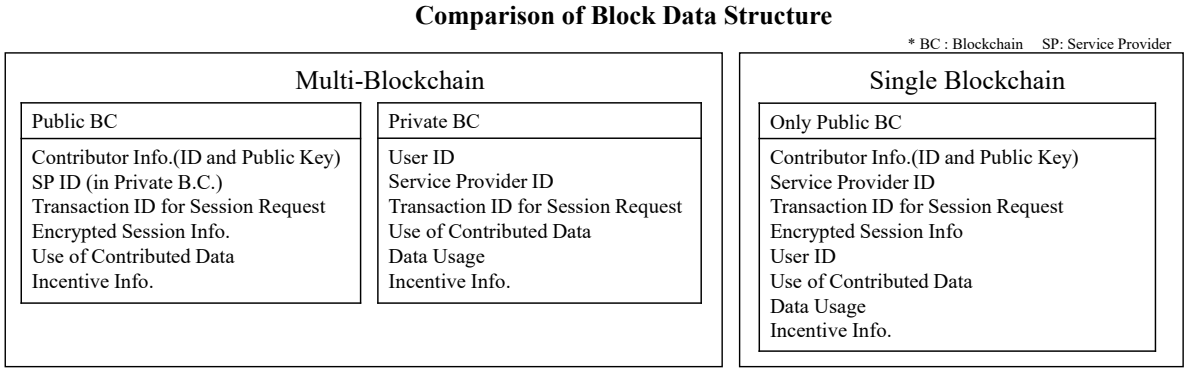

Figure 13. Comparison of block data structure in multi-blockchain and single blockchain.

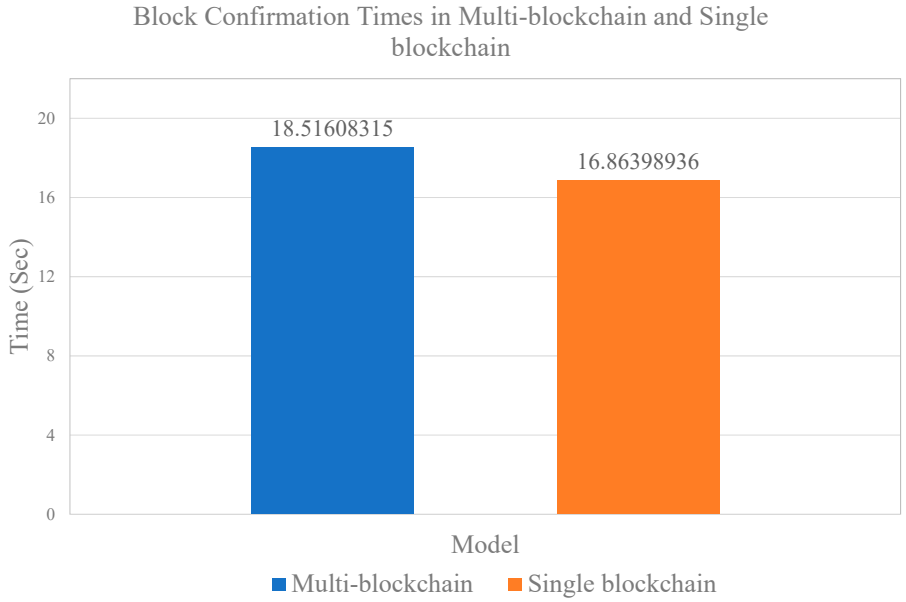

Figure 14. Comparison of transaction confirmation time in multi-blockchain and single blockchain.

5.2. Considerations in Application to Blockchain Mainnet

To analyze the performance of the multi-blockchain structured system proposed in this paper, the execution time and overhead analysis of the main functions were performed with the Ethereum test network (i.e., public blockchain part) and Hyperledger Fabric (i.e., private blockchain part) environment. The environment is a situation where the devices of service providers and all blockchains are not congested.

In this subsection, we consider the congestion situation of the service when the proposed system is applied to the actual operating blockchains (i.e., a large number of users, service providers, and many data contributors participate in the proposed system). In the proposed system, the private blockchain part is only accessible to authorized users and service providers, and it is reported that the actual private blockchains provide a speed of 1000 transactions per second (TPS) or more [27], and 20,000 TPS in the customized fast Hyperledger Fabric [28]. Since the Visa card processing level is 24,000 TPS, a real private blockchain network could support the proposed system at a speed that does not drop significantly compared to the Visa card processing speed.

When the public blockchain part is applied to the Ethereum mainnet, the transaction processing capacity (TPS) is not very high compared to a single server (20 TPS in the case of Ethereum), and the mainnet has to process transactions from other services [29]. That is, assuming the congestion of the service, the performance of the service providers and users may be influenced by the transaction processing capability of the public blockchain. However, if it is applied to a faster public blockchain (e.g., 3000 TPS in EOS [30]) that provides high processing speed, not the Ethereum mainnet, the speed problem can be solved to some extent. In addition, the transaction fee affects the congestion and throughput of the public blockchain [31]. Therefore, in the case of a transaction requiring fast processing, the fee can be adjusted to obtain the performance of the target.

5.3. Security Analysis

The three security advantages of the MCS-based smart parking system constructed on the multi-blockchain structure proposed in this paper are as follows. First, the availability and safety of the smart parking service increases through the use of the public–private blockchains in conjunction. Second, the data contributors enable secure data delivery via transmission of data over a secure session. Third, the reward information for the contributors can also be safely delivered while providing integrity and confidentiality through the blockchains. Each safety feature is described in detail as follows.

Many systems are integrating blockchain technology to provide transparency and safety to information management. The public blockchain provides openness, in the sense that anyone can participate in the formation of the blockchain, and thus it fits well with the characteristics that many data contributors need to participate in the mobile crowdsensing system. However, controlling data access rights or setting restrictions on participation is difficult in the consensus process of block generation. The private blockchain can limit participants, and thus many unspecified participants may be unable to provide the latest sensing values. Therefore, in the system proposed in this paper, data contributors participate in data collection on a public blockchain, with the openness and transparency of information management on the public blockchain assuring the safe delivery of incentive information for reward claims. In addition, the providers and users of the smart parking service can provide access authority processing and safety by allowing only authorized users to participate in service provision and data use through a private blockchain.

Second, the contributors must deliver unstructured data, i.e., photos, to provide data for the MCS system. Even though the contributors remove, as much as possible, any personally identifiable information contained in the photos that they will be sending, delivering these unstructured data in the block of the blockchains is still inappropriate, and thus the contributors need a secure session to deliver the data to the service providers. Therefore, in this paper, the request for session information of the contributor is delivered to the service provider though two blockchains, and the session information encrypted with the contributor's public key is safely replied to the contributor.

Finally, the incentive information of the data contributors calculated according to the data evaluation results of service providers and data users should also be safely transmitted. Accordingly, in the proposed system, the information is encrypted with the public key of the contributor and safely transmitted to the public blockchain. When the contributors claim their rewards, they decrypt the encrypted incentive information with their private keys, and receive the reward in cryptocurrency.

6. Conclusions

In this paper, we have proposed a multi-blockchain structure for data management based on mobile crowdsensing technology to build a smart parking system, a representative service for building a smart city. Mobile crowdsensing technology has an advantage in that it does not require high initial costs, such as those for installing IoT sensors, and can collect large amounts of real-time data through the many mobile devices owned by the public. Through the interworking of public–private blockchains, the proposed system is meaningful in that it provides all the advantages of the public blockchain (i.e., persistence of transactions, safety of public key-based cryptographic data delivery, and integrity management of data) and the private blockchain (i.e., agreed service providers can share and manage data more securely). The experimental results have proven that any performance degradation from the interworking of the public–private blockchains was insufficient. As a future study, we intend to analyze the security vulnerabilities of the bridge nodes and conduct research to cope with these problems.

Author Contributions: M.K. and Y.K. completed this work. M.K. organized the designing and developing the proposed system in this work, and focused on writing the paper. Y.K. implemented and experimented on the prototype of the proposed system. M.K.guided this whole work as a corresponding author. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (number 2018R1A2B6009620).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Schaffers, H.; Komninos, H.; Pallot, M.; Trousse, B.; Nilsson, M.; Oliveira, A. Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation. *Future Internet Lect. Notes Comput. Sci.* **2011**, *6656*, 431–446.
2. Mudaliar, S.; Agali, S.; Mudhol, S.; Jambotkar, C. IoT Based Smart Car Parking System. *Int. J. Sci. Adv. Res. Technol.* **2019**, *5*, 270–272.
3. Chen, X.; Liu, N. Smart parking by mobile crowdsensing. *Int. J. Smart Home* **2016**, *10*, 219–234. [CrossRef]
4. Nãsulea, C.; Mic, S.-M. Using Blockchain as a Platform for Smart Cities. *J. E-Technol.* **2018**, *9*, 37–43.
5. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
6. Wang, J.; Li, M.; He, Y.; Li, H.; Xiao, K.; Wang, C. A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications. *IEEE Access* **2018**, *6*, 17545–17556. [CrossRef]
7. Go Ethereum. Available online: https://geth.ethereum.org/ (accessed on 17 April 2020).
8. Hyperledger Fabric. Available online: https://www.hyperledger.org/projects/fabric (accessed on 17 April 2020).
9. Boubiche, D.E.; Imran, M.; Maqsood, A.; Shoaib, M. Mobile crowd sensing–Taxonomy, applications, challenges, and solutions. *Comput. Hum. Behav.* **2019**, *101*, 352–370. [CrossRef]
10. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 17 April 2020).
11. Introduction to Smart Contracts—Solidity 0.5.8 Documentation. Available online: https://solidity.readthedocs.io/en/v0.5.8/introduction-to-smart-contracts.html (accessed on 17 April 2020).

12. Lin, J.; Li, M.; Yang, D.; Xue, G. Sybil-Proof Online Incentive Mechanisms for Crowdsensing. In Proceedings of the IEEE Infocom 2018-IEEE Conference on Computer Communications, Honolulu, HI, USA, 15–19 April 2018; pp. 2438–2446.
13. Nguyen, G.-T.; Kim, K. Survey about Consensus Algorithms Used in Blockchain. *J. Inf. Process. Syst.* **2018**, *14*, 101–128.
14. Xu, X.; Pautasso, C.; Zhu, L.; Gramoli, V.; Ponomarev, A.; Tran, A.-B.; Chen, S. The Blockchain as a Software Connector. In Proceedings of the 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), Venice, Italy, 5–8 April 2016; pp. 182–191.
15. Chen, Z.; Yu, Z.; Duan, Z.; Hu, K. Inter-Blockchain Communication. In Proceedings of the 2nd International Conference on Computer Science and Technology (CST), Guilin, China, 26–28 May 2017; pp. 448–454.
16. Kan, L.; Wei, Y.; Muhammad, A.H.; Siyuan, W.; Linchao, G.; Kai, H. A Multiple Blockchains Architecture on Inter-Blockchain Communication. In Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16–20 July 2018; pp. 139–145.
17. Wang, Z.; Hu, J.; Lv, R.; Wei, J.; Wang, Q.; Yang, D.; Qi, H. Personalized Privacy-Preserving Task Allocation for Mobile Crowdsensing. *IEEE Trans. Mob. Comput.* **2019**, *18*, 1330–1341. [CrossRef]
18. Wang, J.; Liu, Z.; Tian, X.; Gan, X.; Guan, Y.; Wang, X. Incentivizing Crowdsensing with Location-Privacy Preserving. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 6940–6952. [CrossRef]
19. Jin, H.; Su, L.; Xiao, H.; Nahrstedt, K. Incentive Mechanism for Privacy-Aware Data Aggregation in Mobile Crowd Sensing Systems. *IEEE/ACM Trans. Netw.* **2018**, *26*, 2019–2032. [CrossRef]
20. Jin, H.; Su, L.; Xiao, H.; Nahrstedt, K. Inception: Incentivizing privacy-preserving data aggregation for mobile crowd sensing systems. In Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '16), Paderborn, Germany, 5–8 July 2016; pp. 341–350.
21. Yun, J.; Kim, M. Smart Parking System Using Mobile Crowdsensing: Focus on Removing Privacy Information. In Proceedings of the Korea Information Processing Society Conference, Seoul, Korea, 10–11 May 2018; pp. 32–35.
22. Kim, M.; Yun, J. Saturation Prediction for Crowdsensing Based Smart Parking System. *J. Inf. Process. Syst.* **2019**, *15*, 1335–1349.
23. Ropsten Ethereum Faucet. Available online: https://faucet.ropsten.be/ (accessed on 17 April 2020).
24. The Leading Operating System for PCs, IoT Devices, Servers and the Cloud, Ubuntu. Available online: https://ubuntu.com/ (accessed on 17 April 2020).
25. Ethereum Average Block Time Chart. Available online: https://etherscan.io/chart/blocktime (accessed on 17 April 2020).
26. 4 Cryptocurrencies with Much Faster Block Times than Bitcoin. Available online: https://themerkle.com/4-cryptocurrencies-with-much-faster-block-times-than-bitcoin/ (accessed on 17 April 2020).
27. Thakkar, P.; Nathan, S.; Viswanathan, B. Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform. In Proceedings of the 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), Milwaukee, WI, USA, 25–28 September 2018; pp. 264–276.
28. Gorenflo, C.; Lee, S.; Golab, L.; Keshav, S. Fastfabric: Scaling hyperledger fabric to 20000 transactions per second. *arXiv Preprint* **2019**, arXiv:1901.00910.
29. Bez, M.; Fornari, G.; Vardanega, T. The scalability challenge of ethereum: An initial quantitative analysis. In Proceedings of the IEEE International Conference on Service-Oriented System Engineering (SOSE), San Francisco East Bay, CA, USA, 4–9 April 2019; pp. 167–176.
30. AnTy. Founder Dan Larimer Says EOS Blockchain Can Process 1,000 Sustainable TPS and Up to 3,000 in All. 2019. Available online: https://bitcoinexchangeguide.com/founder-dan-larimer-says-eos-blockchain-can-process-1000-sustainable-tps-and-up-to-3000-in-all/ (accessed on 14 May 2020).
31. Pierro, G.A.; Rocha, H. The Influence Factors on Ethereum Transaction Fees. In Proceedings of the IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), Montreal, QC, Canada, 27 May 2019; pp. 24–31.