Mobile charger billing system using lightweight Blockchain

Nam Ho Kim, Sun Moo Kang, Choong Seon Hong
Department of Computer Science and Engineering
Kyung Hee University, 446-701
Republic of Korea
{knm1471, etxkang, cshong}@khu.ac.kr

***Abstract*— Green transportation such as electric vehicles are emerging as an alternative to the traditional vehicles primarily due to the increasing cost and need of petroleum energy worldwide. These electric vehicle operate by using electric charging and the way to charge an electric car is to use a mobile charger or use a charging infrastructure. Therefore, when a mobile charger is used, a billing system is required through which a user is billed who has charged the electric vehicle. In this paper, we propose a mobile charger billing system that utilizes Blockchain technology. This technology has been applied to achieve more secure online transactions in a peer-to-peer manner. Moreover, we analyze the requirements of mobile charger for billing and propose a lightweight scheme that can overcome the challenge of data size in existing Blockchain.**

Keywords—Mobile Charger, Electric Vehicle, Blockchain, billing, Lightweight

I. Introduction

Recently, consumption of petroleum energy has increased worldwide, and the amount of petroleum consumed by automobiles has reached up to 30% of the total consumption. Therefore, it is recommended to find alternatives and use green transportation such as hybrid electric vehicle (HEV) and electric vehicle (EV).

According to [2] and [3], the global market for electric vehicles in 2015, including EVs, has reached 550,000 units. In North America, most electric vehicles are mainly charged at home. Benz and BMW, for example, are helping to set up a charging points for each home when buying their own electric car. However, in populated places where there are no garage, it is difficult to install a charge point. Also, If garage is shared among a building, the billing must be made to the concerned person, i.e., who has charged his car rather than divide equally. Therefore, in order to grow and disseminate the electric vehicle industry, it is necessary to devise an infrastructure and appropriate methods to solve these aforementioned issues.

Typically, there are two main methods for charging the electric vehicles, one uses a charge point while the other uses a mobile charger. If a charge point used, it will charge the electric vehicle using a grid-based fixed charging infrastructure. In case of mobile charger, the vehicle is charged from a power supply device by using the mobile charger.

In the case of using a mobile charger, it is important not only to charge the electric car, but also to impose a cost to the user who charges the electric car. If a user charges an electric vehicle from a power supply at a place other than his / her home, there is probability that the billing is imposed on a person who is the owner of that place and not to the person who has charged the electric vehicle. Furthermore, charging at public places further complicates the scenario in which it becomes almost impossible to identify exactly who charged the electric car. Therefore, the current international standard for mobile charging for electric vehicles is insufficient and has a number of open issues which need to be addressed. One of them is to establish a policy on how to impose the billing to the actual users.

The transaction on the Internet have been dependent on financial institutions. However, if you depend exclusively on financial institutions, it will suffers from the inherent weaknesses of the trust-based model. Thus, there is a need for an electronic payment system for direct transactions between trading partners, without the existence of a trusted third party. In this work, we proposes a mobile charging billing service system using Blockchain to solve the aforementioned scenario. Blockchain is a technique that enables reliable electronic transactions by creating computational evidence of the time sequence of transactions using a peer-to-peer distributed timestamp server to solve this problem [4].

The rest of this paper is organized as follows: In Section II, we provide detailed related works for understanding the proposed system. Then, we describes the proposed system with its architecture in Section III. Section IV analyzes the performance of our proposed system. Finally, we conclude and discuss our future work in Section V.

II. Related Work

A. Blockchain

Current online transaction rely on certain trusted institutions. However, these third party sources can be hacked, manipulated or compromised [5]. Thus, novel secure schemes are required.

In 2008, Nakamoto Satoshi proposed the Blockchain technology to solve the above problems. They explain electronic cash which is dealt in peer-to-peer network so that direct transactions can be made between the two parties without trading through a third trusted institution. A Blockchain is essentially a public ledger that is executed and shared between participants. Once the data has been entered into the block, it is difficult to forge or delete the information. If a malicious user attempts to modify or delete a block, it must also modify all previous blocks as well as the block at that point in time. Figure 1 shows an example of an online transaction using Blockchain.

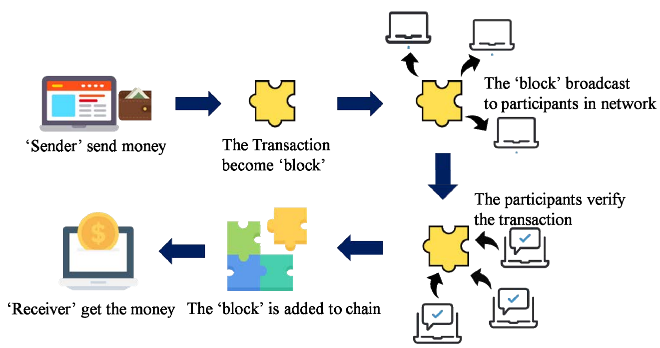

Figure 1. Example of the How to Blockchain works

Each Blocks constituting a Blockchain consist of a 'block header' and a 'block body'. The block header includes the hash value of the previous block header. In addition, each block is linked by a linked list method such as a chain. Block bodies may contain different values depending on its service.

B. SPV(Simplified Payment Verification)

Note that all nodes do not possess the capability to store the full Blockchain especially the resource constrained devices, e.g., space and power-constrained devices cannot maintain the full Blockchain. Therefore, for such devices, a simplified payment verification (SPV) is used to operate without the full Blockchain. SPV nodes download only the block header rather than the complete chain. Therefore, they do not know about the transactions.

SPV nodes can verify the transactions using a different method. They verify transactions by reference to their depth in the Blockchain instead of the height. SPV nodes will verify the chain of all blocks and link that specific chain to the transaction of interest [6]. The SPV node will establish a link between the transaction and the block that contains it, using a Merkle Path (details of Merkle tree explained in next subsection).

III. Scenarios and System Architecture

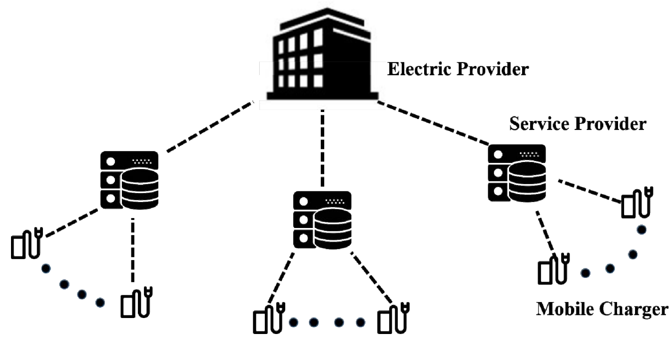

Figure 2. System Model

Fig 3 shows our system model. The system consists of a power supplier, a service provider, and a mobile charger. It is assumed that both the Service Provider and the mobile charger parent node are Full Block. The remaining mobile chargers utilize SPV. In this section, we propose a data structure of a mobile charger for charging through a mobile charger, and discuss how to make lightweight Blockchain.

A. Mobile charger packet information for billing

Before referring to the mobile charger packet information for billing according to its charging, it is assumed that each mobile charger knows the IP address of its own service provider. If each mobile charger is operated on the network for the first time, it can only participate if it searches other nodes in the network. As this time, each mobile charger can obtain the information of the current block and the neighboring node through the service provider.

We shows the message type and data type of the mobile charger. Table 1 shows the message type whereas the data types are specified in Table 2. If some users make charging group and pay the charging fee at the same time, it is much more effective to impose one charger group than to charge for each mobile chargers. Furthermore, some person group can pay the charging fee at the same time, this case is same as like the previous case. Therefore, the mobile charger can have a 'groupId' value with a unique identifier. If certain mobile chargers are grouped together, they can be grouped by passing their groupId value to their service provider.

TABLE I. Message Type

Message	Description
Register	The mobile charger registers itself by transferring its 'idTag' to the Service Provider Server. If grouping is required, the 'groupId' value can be passed along with the idTag value.
RegisterAck	Response message to 'Register'.
CheckAuth	If a new mobile charger is added to the group, the Service Provider server forwards this message to the parent node of the group. After receiving this message, the mobile charger confirms that the idTag value of the charger to

	be added belongs to its own group.
CheckAuthAck	Response message to 'CheckAuth'
Authorize	A mobile charger participating in a group requests permission to join the group by sending its idtag.
AuthorizeAck	Response message to 'Authorize'

TABLE II. DATA TYPE

Type	Description
idTag	**Mobile Charger unique identifier**
idTagInfo	**It is delivered after registration. There are 'Interval', 'currentTime', 'status' fields. 'status' field is used only when making a group, and if it has an Accepted, it means the mobile charger get authority to the group**
Interval	**Cycle to send 'ChargeProfile'**
currentTime	**The current time in the Service Provider. It is used to synchronize the mobile charger's internal clock**
ChargeProfile	**Charge history of mobile charger. It consists of idtag and each charge history. Charging history includes start time, maximum output power, and end time.**

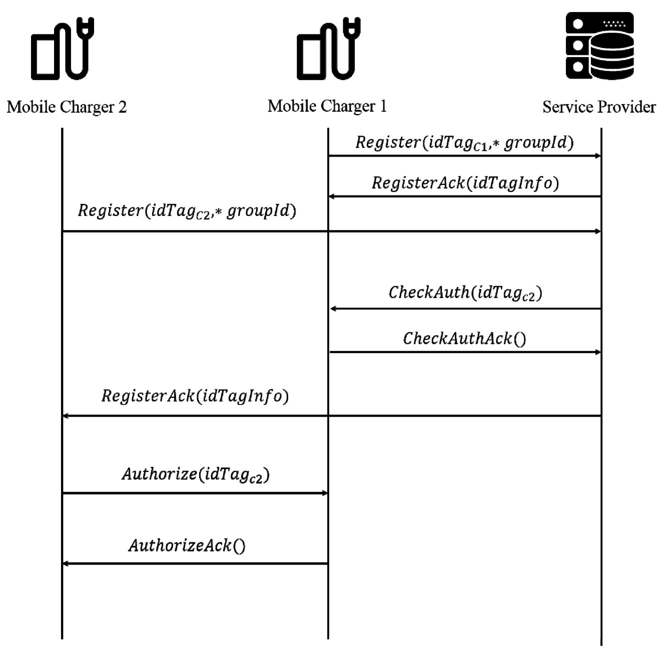

Figure 3. Sequence of the mobile charger registration

Figure 4 shows the sequence for making group of multiple mobile chargers. Each message and description is shown in Table 1. Each groupId value is unique, and the first mobile charger to register groupId serves act as the 'parent node' of the group. In the proposed system, the parent mobile charger is a full node(all blocks are held), and the other mobile charger in the group is an SPV node.

After completing the registration sequence with the Service Provider, the mobile charger transmits its Charging Profile to the Service Provider after completing the charging process. If the service provider receives 'Charging Profile' from mobile charger, it sends the 'Charging profile' to chargers belonging to other group. The mobile charger delivers all its charging profiles which occurred within the 'interval' value from idTagInfo to the parent node. The parent node that receives the profile of the group generates a block containing the contents of all profiles and sends it to the service provider. The Service Provider forwards the block to all groups. If you get more than half the correct validation results for a transaction, the service provider adds the block to the existing Blockchain. Then Service Provider pass the block to all nodes. The service provider checks the block information for billing and transmits the charge information according to the charge amount for each group.

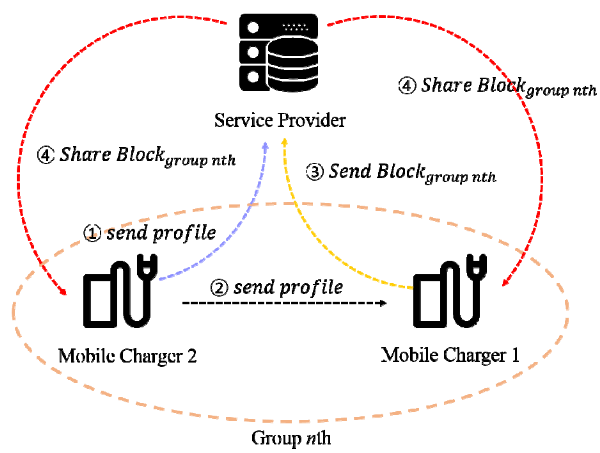

Figure 4. Sequence of transaction communication

B. *Lightweight Blockchain data*

Currently, the Blockchain technique has some limitations. One of the biggest challenge in it is the size of the data. The Blockchain will continue to accumulate previous data records, so the size of the data over time will increase. Moreover, in Blockchain architecture the data is generated after every pre-determined period and this data is broadcasted to all node that belong to the network. So, if the number of nodes are increased, the data size will grow exponentially. Thus the cost of maintaining this data will also increase accordingly.

To reduce the size of the data, a simple way is to delete the old block data which are no longer needed and not required to be maintained. However, this method may cause another issue relating to the loss of the data value at a certain time. For example, since the previous charge record is deleted, the user may deny the its bill even though the charge was actually made by the user.

Algorithm 1 : Block Data Size decrease

Input: $\boldsymbol{Whole\ Block}$
Output: $\boldsymbol{Charge\ List\ Block}$
Check Charging Data for each group
    for number of group do
        $CurrentBlockCharge$ per each group is '0'
    end for
    do
        for number of group do
            $i = 1$
            $Charge_{G_i} = Charge_{G_i} + CurrentBlockCharge_{G_i}$
        End for
        $CurrentBlockCharge$ move to next Block
    while(End of Block)
Generate Charge List Block
    for number of group do
        Add $Group_{id} + Charge_{G_i}$ to *Block data*
    end for
    Add $BlockHeader_{lastest}$ and $Block\ data$
    Send *Charge List Block* to each group parent node

In our proposed scheme, parent mobile charger maintains the full Blockchain and other mobile chargers in the group are SPV node. In such case, any charger may be reluctant to become a parent node as the parent mobile charger have to maintain an additional overhead of the full block. So, we propose a novel method to reduce Blockchain data size for parent node. The proposed method makes more efficient management compared to the block data. The proposed method is a re-construction of a block into a new type of block which is called Charge List Block. The service provider receives block for each group transaction from the parent node, and it re-constructs the block body part. The service provider periodically checks the size of the Blockchain data received from each group. If the size of the Blockchain data exceeds a certain size, it check the billing profile for the last transaction for each group. The Service Provider checks the height of the block from the first block to the block containing the last transaction contents. After this process, the Service Provider creates a Charge List Block by listing the idTag and charge usage of all mobile chargers in the group. The block header of the Charge List Block is generated in the same way as the existing block header part, and is transmitted for each group. The group parent mobile chargers receive the newly created block form a new Blockchain starting from the reconstructed block. Through this method, the parent mobile charger can be maintained the lightweight full Blockchain.

IV. Performance Analysis

In this section, we present the results of our analysis for the proposed method of mobile chargers and the lightweight Blockchain technique.

If any malicious user wants to change the existing charging record, he or she must change not only that block but also all blocks after that block. In fact, it is impossible to change the record because it is shared by all nodes participating in the network.

Since the parent node receives the profile in the group of every interval, the malicious user may attempt to change the value of the profile in the group on the parent node. However, such an attack can be detected as in the above example. This is because, if the parent node changes the value to generate a block, the nodes belonging to the other group receive the existing profile contents in advance, and can confirm whether or not the profile is changed through validation. If the contents of the profile are different, the block containing the profile is not tied to the existing Blockchain. Therefore, it is impossible to attack a profile change with malicious parent.

The proposed lightweight Blockchain scheme can reduce the size of existing Blockchain data. Existing blocks must include a signature and a secret key for each transaction. However, if the proposed method is used, the data size can be greatly reduced because only the idTag, the charging amount of the mobile charger and the hash of the last transaction are maintained even if the number of transactions increases.

V. Conclusion and Future work

In this paper, we propose a mobile charger billing system using Blockchain. In order to provide efficient charging according to the charge details of the mobile charger, the mobile charger can be grouped by utilizing the groupId. In addition, using Blockchain technology, appropriate billing for charging can be generated. Moreover, we propose a technique to reduce the size of block data, and solve the problem of accumulating data size of existing Blockchain.

However, in the proposed system, there is still remains a challenge that needs to be addressed. It is possible for a particular attacker to pretend to have a lot of mobile chargers. Therefore, when validating a block, an attacker can send a lot of messages that block is not valid. In such a case, the block may not be added to the chain, even if the block is valid, according to the principle of a block chain. Therefore, we intend to further study more techniques to address this problem as future research course.

Acknowledgment

This work was supported by the Industrial Strategic Technology Development Program(10067093, Development of the Communication Standards and the Regulations of Electrical safety for the Portable Charger) funded By the Ministry of Trade, Industry & Energy(MOTIE, Korea). *Dr. CS Hong is the corresponding author

References.

[1] Sangkyu Lee, Daewoong Han, Gubae Kang, Seongyeop Lim, "Research for improvement of charging system efficiency on Electric Vehicle", 2013 KSAE(The Koreaan Society of Automotive Engineers) conference, 1887-1892

[2] A. Y. Saber and G. K. Venayagamoorthy, "One million plug-in electric vehicles on the road by 2015", 12th International IEEE conference on Intelligent Transportation System, USA, Oct 2009, pp 141-147

[3] Autonomous car and electric car trend report, NRT Corporation,

[4] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008

[5] Michael Crosby et al, Blockchain Technology: Beyond Bitcoin. AIR(Applied Innovation Review), June 2016, No. 2

[6] Andreas M. Antonopoulos LLC. "Mastering Bitcoin : Unlocking Digital Cryptocurrencies".