Blockchain based Billing System for Electric Vehicle and Charging Station

Seohyeon Jeong, Nhu-Ngoc Dao, Yunseong Lee, Cheol Lee and Sungrae Cho
School of Computer Science Engineering
Chung-Ang University
221 Heukseok, Dongjak
Seoul, South Korea
{shjeong, dnngoc, yslee, clee}@uclab.re.kr, srcho@cau.ac.kr

***Abstract*— Research related to electric vehicles (EVs) is mainly focused on hardware such as battery charging method, and there is still a lack of software (service oriented) research such as billing system that needs to be developed realistically. The result of the charge measured in the charging EV can be different from the charge amount claimed to be charged in the charging station. This is because the charge is measured separately from each other using its smart meters. And if mechanical measurements are assumed to be accurate, it is possible to lie in one of the EV or charging station. Also, billing information can be manipulated. To prevent those problems, this paper proposes the blockchain based billing system. The EV and the charging station store the billing information in the blockchain after mutual authentication and prevent the modification. A blockchain is the system in which all nodes have the same ledger, therefore cannot be tampered with. This prevents a user from modifying the record after charging.**

Keywords—blockchain; billing system; electric vehicle; charging station;

I. INTRODUCTION

With the need for environmentally green energy, supply of electric vehicles (EVs) is increasing in popularity. The spread of EVs led to the development of EV's battery charging technologies. Currently there are various charging methods in wired/wireless charging modes. EV charging technologies are evolving day by day [1], [2]. However, the development of the technologies is mainly performed in the hardware part of the charging field, and there is not yet a software study on the secure billing system which is essential. The present billing system is briefly performed in following process. The charging station requests payment to the credit card company with the billing information (i.e., EV user's card information, charging fee) provided by the EV user and charging station, after the charging station charged to the EV. At this time, the EV or charging station can provide fault information, which may result in invalid billing. For example, the charge profile measured at the EV can differ from the charge amount provided from the charging station. This can happen because EV and charging station measure the charge amount with their own measurement equipment. Therefore, the EV or charging station can intentionally manipulate the charging information, which can cause confusion in the contractual relationship between EV and charging station.

A blockchain was introduced in 2008 by Nakamoto Satoshi to make a Bitcoin [3]. The blockchain is a technique that uses a distributed ledger based on a hash function, enabling the transaction of trustless nodes without a trusted third party. The current blockchain technology is being considered for the application of the whole society beyond the field of cryptocurrency. Particularly, research on the application in the authentication field and in the form of a contract called the smart contract is actively performed. Based on the hash value contained in the block and having the same ledger for every node, the blockchain can prevent forgery in the untrusted relationship also it is possible to know when the ledger is forged by the certain node.

In here, the mutual authentication between the EV and the charging station is based on the terms of their transaction and permits the authorization when the terms of the transaction meet the interests of each other. The authorization of the certification is confirmed by sharing the same ledger and writhe the transaction. The failure of the mutual authentication means that the transaction is not agreed by one's side.

In this paper, it is assumed that the EV and the charging station, which can record different amounts of the charge, are mutually untrustful. The ledger with transactions of the blockchain provide the secure billing system by sharing non-modifiable block.

II. SYSTEM ARCHITECTURE AND MODEL

The billing system is used for electricity trading between the EV and charging station. The EV and charging station each have a communication entity and a power management entity. Also the communication entity can exchange information by wireless communication under various communication situations [4]-[6].

A. EV Nodes

EV nodes are the electric vehicle nodes that want to purchase electric power from the charging station. There are battery management and communication entities in the EV. EV nodes can either purchase energy, generate a block, or idle. If

This research was supported by Korea Electric Power Corporation (Grant number: R17XA05-43).

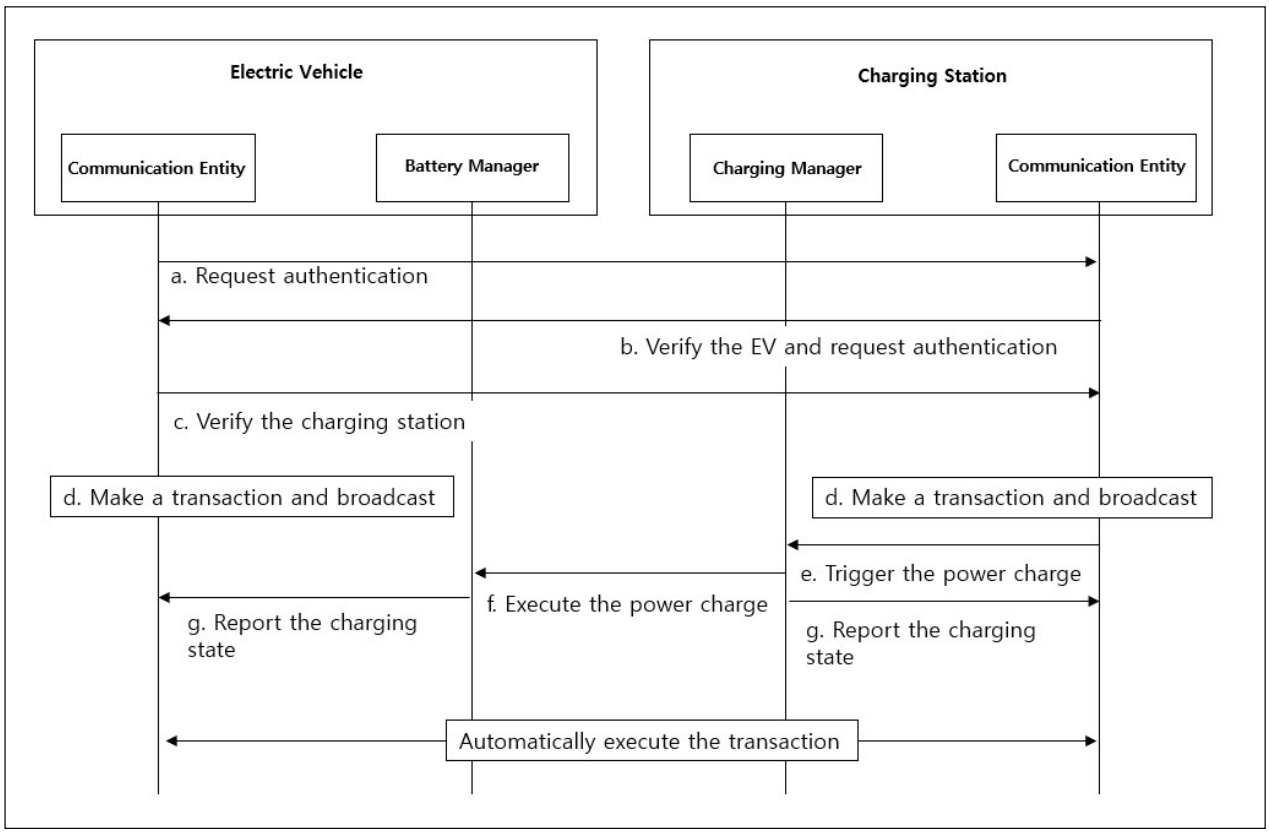

Fig. 1. The brief process of the entire system

the EV agrees to trade with charging station, it can write the transaction with the requirements and information to the block.

B. Charging Station Nodes

Charging station nodes want to sell electricity power to the EV nodes. Charging management and communication entity exist in the charging station nodes. Charging station nodes can either sell power, generate a block, or idle. If the charging station nodes agrees to sell the power to the EV, it can write the transaction with the trading information and requirements.

C. Minor node

Among the EV and the charging station nodes, the miner node is responsible for generating blocks. The miner node is selected as the node with the highest transaction history among the relative node with the EV and the charging station to be traded.

D. Battery Managemer and Charging Managemer

Each of battery manager and charging manager is the part that manages the smart meters inside EVs and charging stations. It calculates the amount of the power to be charged and report it to each communication entity. When charging is completed, the EV informs charging station through the communication entity. The charging station verify it and compares it with its charge amount. The EV and charging station then broadcast the completion of the charge so that the transaction can be executed via the communication entity.

E. Communication Entity

Communication entity plays a similar role in the EVs and charging station. It requests the latest blockchain on the network before trading. Also, it broadcast the transaction details to the network. The communication between the EV and the EVSE that wants to deal is also done in this part. The information of the trading and measured charge amount of each other are main contents. As a completion of the charging, their result reported by the battery management and the energy management are broadcast to the network and execute the remained transaction.

III. SMART BILLING SYSTEM

A. Mutual Authentication

In the absence of a trusted third party, mutual authentication between EV and charging station is essential. Prior to authentication, EV and charging station that want to

make transaction have to connect to the network to create new public and private key pairs. The key pair is generated using the Elliptic Curve Digital Signature Algorithm (ECDSA) [7]. After generating each key pair, its own device ID and public key can be shared, then it can be assumed that EV and charging station know each other's public key and device ID. We also use SHA256 as a hash function in the proposed system.

After the mutual authentication is done, the same transaction can be created for both side and broadcast to the network for inclusion in the block. Fig. 1. shows this process briefly.

B. Blockchain

Blocks are written in a programmable script language. The block contains the transaction list, hash value of the previous block, serial number, miner's ID, and miner's signature. The global reputation includes EVs ID, charging stations ID, transaction history for each node. The transaction list is a list of contracts created by EVs and charging stations that are currently in trading. The serial number is a unique number of the block and is incremented by 1 each time a block is generated. The miner's ID should be recorded with the miner signature as the ID of the miner that created the block. The miner's signature is the result of signing the block with its secret key, which allows other nodes to evaluate the validity of the miner. In this paper, it is assumed that only nodes with a length of transaction history which is greater than or equal to a constant length $\boldsymbol{L}$ can be miner nodes. Mining is performed once at time $\boldsymbol{T}$. In bitcoin, this time corresponds to the time set in 10 minutes. It can be set to less than 10 minutes for the characteristics and convenience of the transaction.

The miner collects and verifies the information reported by EV and the charging station after the trading, and generates a block containing the results and broadcasts it to the network. The newly created block has to be updated the serial number and include the ID and signature of the miner node.

C. Transaction

The EV and the charging station have to report their charging status at each transaction. The reports are always recorded in the block, and the blocks forming the chain cannot be manipulated, so that the record of each other cannot manipulate the previous history. Also, the reliability of the billing system improves as the chain becomes longer. For a billing system, an identified transaction address *txAddr* has to be created by the EV and charging station. Then transaction is created at this *txAddr*. The content of the code at *txAddr* cannot be modified after it has been created. The EV and the charging station can inquire the contents of the transaction through queries or trigger the execution of the code with commands [8].

IV. Conclusions and Future Directions

As the spread of EV increases, there is a need to develop technology not only for charging technology but also for related services. In this respect, we propose a blockchain-based billing system for reliable transactions between various charging stations and vehicles that are not mutually trustworthy. It can prevent manipulation of billing information when billing is performed after charging phase. It is expected that a further developed billing system will be build up later by combining various proof of work and current novel encryption algorithms. Also, there is an authentication protocol in peer aware communication (PAC) which is similar with traditional authentication schemes [9], [10]. When a node accesses the network, such an authentication protocol can be combined to provide greater security.

Acknowledgment

This research was supported by Korea Electric Power Corporation (Grant number: R17XA05-43).

References

[1] F. Musavi and E. Wilson, Young, “Overview of wireless power transfer technologies for electric vehicle battery charging,” IET Power Electronics, vol. 7, pp. 60-66, January 2014.

[2] C.C. Hua and M. Y. Lin, “A study of charging control of lead-acid battery for electric vehicles,” in Proceedings of the 2000 IEEE International Symposium on Industrial Electronics (ISIE), Puebla, Mexico, December 2000.

[3] S. Nakamoto, “Bitcoin: A peer-topeer electronic cash system,” 2008. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[4] W. Na, Y. Lee, J. Yoon, J. Park, and S. Cho, " Fully-Distributed Multicast Routing Protocol for IEEE 802.15.8 Peer-Aware Communication," International Journal of Distributed Sensor Networks, vol. 11, no. 8, August 2015.

[5] W. Na, G. Lee, H. Bae, J. Yu, and S. Cho, " Reliable Broadcast Scheme for IEEE 802.15.5 Low-Rate WPAN Mesh Networks," IEICE Transactions on Communications, vol. E95-B, no. 09, pp. 2700-2707, September 2012.

[6] W. Na, Y. Lee, J. Yoon, J. Park, and S. Cho, " Fully-Distributed Multicast Routing Protocol for IEEE 802.15.8 Peer-Aware Communication," International Journal of Distributed Sensor Networks, vol. 11, no. 8, August 2015.

[7] D. Johnson, A. Menezes, and S. Vanstone, “The elliptic curve digital signature algorithm (ECDSA),” International Journal of Information Security, vol. 1, no. 1, pp. 36-63, July 2001.

[8] K.Christidis and M. Devesikiotis, “Blockchains and smart contracts for the internet of things,” IEEE Access, vol. 4, pp. 2292-2303, May 2016.

[9] Y. Kim, N. N. Dao, J. Lee, and S. Cho, “Trend analyses of authentication in peer aware communication (PAC),” in Proc. of Ubiquitous and Future Networks (ICUFN), Milan, Italy, July 2017.

[10] N.-N. Dao, Y. Lee, S. Cho, E. Kim, K.-S. Chung, C. Keum, "Multi-tier Multi-access Edge Computing: The Role for the Fourth Industrial Revolution," in Proc. of ICTC, Jeju, Korea, October 2017