A Blockchain-Based Electric Vehicle Charging Cooperation Model

Soojin Lee, *Student Member, IEEE*, Seung-Hyun Seo, *Member, IEEE*, Kyubyung Kang, *Associate Member, IEEE*, and Qin Hu, *Member, IEEE*

***Abstract*—Due to the rising number of Electric Vehicles (EV), the subsequent increase in demand for charging, as well as the long charging time, will make it difficult for drivers to charge their vehicles. Current charging service platforms inform their customers of the charging station information for the network to which they belong. However, they do not ensure the reliability and credibility of information and do not share the charging information of other charging stations. To address this issue, a model in which CSs collaborate for information sharing and charging must be developed. In this paper, we propose a blockchain-based integrated charging platform for charging cooperation. Verifier groups for each CS verify the reliability of shared information. We applied the concept of Mobile Charging Stations (MCSs) to help busy CSs, reducing EV charging latency. We also designed a contribution-based incentive distribution process to elicit active CSs' cooperation. We performed a charging scenario simulation and blockchain implementation to demonstrate the proposed model's efficacy. The simulation results showed that the proposed charging scenario with MCS application showed a 46.9 % reduction in waiting time. Also, when the number of verifier members equals the global average of EVs per charging spot, the verification time is approximately 547 ms, demonstrating that the proposed model is effective.**

***Index Terms*—Electric vehicle, blockchain, charging system, data sharing.**

I. Introduction

ACCORDING to Statista [1], the number of autonomous vehicles is steadily increasing, and it is expected to reach 54 million worldwide by 2024. Additionally, the market for self-driving electric vehicles, falling under the category of autonomous vehicles, is expected to show an average annual growth rate of 36.3 % from 2022 to 2031, and the market size is anticipated to reach 5000 billion dollars [2]. Self-Driving Electric Vehicles (SDEVs) are equipped with communication technology, advanced artificial intelligence algorithms, and sensor technologies, enabling them to communicate with each other and make autonomous decisions. The proliferation of SDEVs plays a significant role in advancing intelligent transportation systems.

SDEV can communicate with electric vehicle service providers and surrounding vehicles to exchange necessary data, which enables them to select charging stations. For instance, SDEV drivers obtain various kinds of information regarding the locations of nearby charging stations, the status of charging equipment, such as whether chargers are malfunctioning, charging costs, and real-time availability of charging stations [3]. Moreover, they receive real-time traffic information from surrounding vehicles [4]. Drivers can select charging stations that meet their preferences and requirements based on the shared information. However, malicious attackers can disseminate incorrect information and interfere with drivers' optimal choices. According to [4], vehicles share traffic information with other vehicles through Basic Safety Messages (BSM). At this time, a malicious attacker can falsify or manipulate the information in the BSM to prevent the vehicle from selecting the correct driving route. Misinformation in traffic systems can manipulate driving routes and cause traffic disruption by influencing drivers' decisions [5].

Many studies have investigated methods to securely share data between autonomous vehicles and stakeholders [6], [7], [8]. However, enhancing the reliability and credibility of sharing information between charging stations and self-driving EVs has not been sufficiently investigated. False charging station information may hinder the selection of the optimal vehicle charging station. It also can affect the overall traffic system since shared EV charging station information impacts traffic flow, depending on which charging stations EV drivers choose [9]. If attackers disseminate fake charging station information, they could execute divergence attacks, directing EVs away from specific locations or convergence attacks, causing EVs to gather at particular places [5]. In other words, they might disrupt operations at charging stations or, conversely, manipulate vehicle movements to maliciously increase the profit of a specific charging station. Thus, it's essential to prevent the propagation of fake charging station information to maintain a stable traffic system.

In addition, EV drivers have range anxiety, which means that they are concerned that they might not reach their far-off destination due to the EV's battery draining. Various charging service models are being commercialized to reduce drivers'

Received 29 April 2024; revised 8 September 2024; accepted 17 October 2024. Date of publication 6 November 2024; date of current version 5 March 2025. This work was supported by grants from the Institute of Information & Communications Technology Planning & Evaluation (IITP), funded by the Korea government (MSIT): (RS-2023-00225201) Development of Control Rights Protection Technology to Prevent Reverse Engineering of Military Unmanned Vehicles; (IITP-2024-RS-2024-00423071) Convergence Security Core Talent Training Program; and (RS-2024-00341722) Development of Cyber Resilience Methods for Intelligent Service Robots. The review of this article was coordinated by Dr. Zeeshan Kaleem. *(Corresponding author: Seung-Hyun Seo.)*

Soojin Lee is with the Department of Electronic and Electrical Engineering, Graduate School of Hanyang University, Ansan 15588, South Korea (e-mail: tssn195@hanyang.ac.kr).

Seung-Hyun Seo is with the Division of Electrical Engineering, Hanyang University, ERICA Campus, Ansan 15588, South Korea (e-mail: seosh77@hanyang.ac.kr).

Kyubyung Kang is with the Construction Management Technology, Purdue University, West Lafayette, IN 47907 USA (e-mail: kyukang@purdue.edu).

Qin Hu is with the Department of Computer Science, Georgia State University Atlanta, Atlanta, GA 30302 USA (e-mail: qhu@gsu.edu).

Digital Object Identifier 10.1109/TVT.2024.3492393

range anxiety. For example, SparkCharge [10] provides a mobile electric vehicle charging network and delivery charging service by using a mobile app in the US. ChargeHurb [11] guides vehicles to the locations of available charging stations in North America via the ChargeHub map, and users share feedback on specific charging stations through its application. PlugShare [12] is an EV charging information application available worldwide, and it provides public, high-power, or residential charger information. However, these EV charging service models don't share the availability and status of their charging stations. Thus, when long-distance drivers are out of their daily life radius, they need to get the locations and charging information of their desired charging stations. To reduce range anxiety, EVs require the capability to monitor charging traffic and locate an available charging station when needed. Therefore, the development of a new charging information-sharing platform considering multiple Electric Vehicle Service Providers (EVSPs) is essential. In this market circumstance, some EVSPs may not be willing to share infrastructure or charging information to monopolize customers, regardless of charging efficiency. Active participation of EVSPs is required to operate the proposed model effectively. Thus, a practical method to actively motivate EVSP to participate in the charging platform is necessary.

Sharing various types of information between EVSPs using a platform is challenging because EVSPs do not inherently trust each other when they need to share information. Blockchain technology, which is characterized by its decentralization, data integrity, and traceability, can be a good solution for this challenge by promoting EVSPs to share information securely. So far, blockchains have been applied in various fields, including vehicular networks [13], smart governance [14], and so on. It can also play a critical role in sharing and managing charging station information. Through blockchain, Charging Stations (CSs) can securely share information, such as charging bidding, charging matching, charging station state, and availability of stations. Several studies have proposed electric vehicle charging models applying blockchain technology [15], [16], [17], [18], [19], [20]. Wang et al. [15] proposed a blockchain-based model for Private Charging Pile (PCP) sharing. They developed a joint coalition-matching game-theoretical algorithm to match EVs and PCPs. Baza et al. [16] proposed a blockchain-based energy trading scheme for charging station-to-vehicle and vehicle-to-vehicle. To preserve EV's privacy, the authors applied Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (ZK-SNARK) [21]. However, [15] and [16] did not consider the reliability and credibility of transactions stored in a blockchain ledger.

Hence, we propose an integrated EV charging platform that consists of two layered blockchains: a charging traffic volume blockchain and a charging cooperation blockchain. The charging traffic volume blockchain stores charging traffic information reported by participants around each CS to achieve reliable charging information sharing. Verifier group members verify the reliability of reported transactions to prevent false information propagation. To motivate the participation of EVSPs, our model pays incentives to the EVSPs based on the contribution of each CS in the charging cooperation blockchain. The charging cooperation blockchain is a consortium blockchain in which only charging suppliers participate. It stores the contribution value of each CS, transactions between charging suppliers, and incentive distribution results. The proposed platform applied the Shapley value [22] to calculate each CS's contribution value. The Shapley value is a concept that finds the overall contribution by calculating the marginal contribution of each agent for each coalition of agents in the cooperation game. The proposed platform has four contribution factors: a charging number, a charging amount, a charging cooperation number, and a charging amount of charging cooperation. These factors determine the total contribution value of each CS. We employed contribution-based Practical Byzantine Fault Tolerance (PBFT) that assigns greater voting power to CSs with higher contributions, thus allowing them to significantly influence blockchain decisions.

Furthermore, we applied a Mobile Charging Station (MCS) [23], which can alleviate charging bottlenecks and provide charging solutions to long-distance drivers. Charging stations in crowded places such as shopping malls and corporate buildings tend to attract more EVs and cause charging congestion. To reduce charging latency, CSs can send their MCSs to support busy CSs. If there is no nearby CS, drivers can request MCS from CS via the charging traffic volume blockchain. Thus, the use of MCS allows long-distance drivers to drive more efficiently and reduces the charging time of EVs. To demonstrate the benefits of MCS, we simulated a long-distance driving scenario and a public charging points scenario by using Indiana Statewide Travel Demand Model (ISTDM) [24] and charging station information in the state of Indiana. The simulation results show that the proposed model can reduce long-distance drivers' total driving distance, range anxiety, and charging latency at specific public charging points with high charging demand. The overall model is depicted in Fig. 1. The main contributions of this paper are summarized below.

- We propose a new blockchain-based charging cooperation model considering the reliability of charging information to lessen range anxiety. we applied a verifier group to verify the shared information's reliability and credibility by applying verifier groups. The proposed model allows EVs to make optimal decisions for charging based on shared information.
- We design contribution-based practical byzantine fault tolerance to encourage CS's active participation. The history of the CS's charging and cooperation determined the contribution value of the CS. Moreover, by distributing incentives according to their contribution, the model motivates CSs to cooperate with other CSs actively.
- We conducted a simulation of the scenario involving cooperation in EV charging and demonstrated the effectiveness of our model. In addition, we implemented a blockchain prototype and charging matching chaincode to evaluate its performance in comparison to previous works [18, 34]. The experimental results showed that our model reduced transaction overhead and charging latency compared to previous studies [18, 34].

The remainder of the paper is organized as follows. We summarize related works in Section II and explain preliminaries in Section III. Section IV introduces the blockchain-based integrated EV charging platform. We describe the proposed protocol in Section V. In Section VI, we analyze the security of our

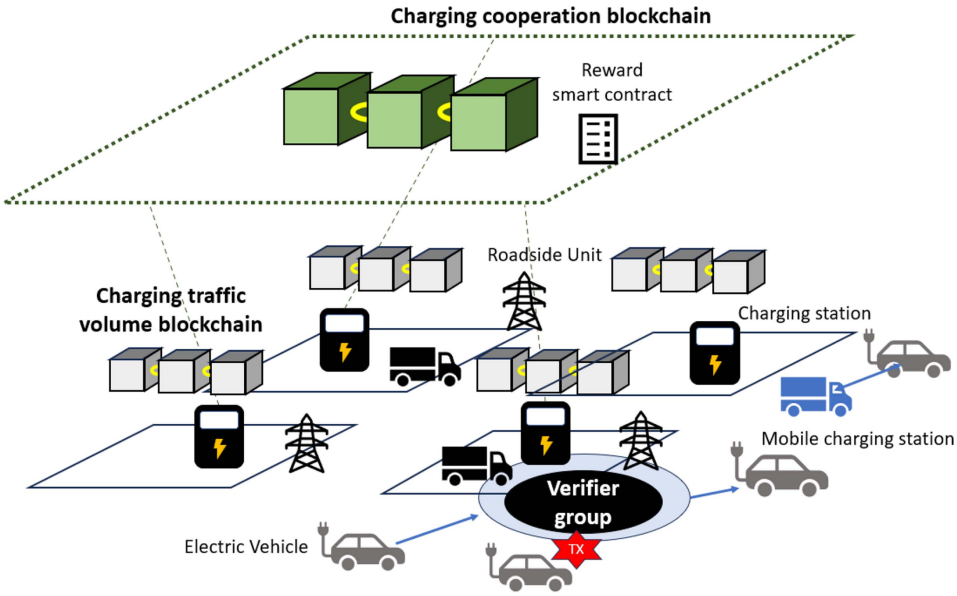

Fig. 1. Overall platform.

platform and show the simulation result. We conclude the paper in Section VII.

II. Related Works

A. Charging Model for Efficient Electric Charging Service

Recently, several researchers have presented methods for vehicles to use an optimal charging station for efficient charging services [25], [26], [27]. Zavvos et al. [25] proposed an optimal charging station selection model considering charging station competition to maximize station investors' profit and minimize travel costs of EV drivers. EVSPs decide the charging station's location, capacity, and charging price using the proposed Subgame-Perfect Equilibria (SPE). Lee et al. [26] proposed an optimal route and charging station selection model by applying deep reinforcement learning. The model minimizes the overall travel time in environments with dynamic charging requests and traffic conditions. Zhou et al. [27] developed an EV charging station location optimization model using a genetic algorithm. The proposed scheme reduces the overall total operating cost of the charging station and selects the optimal charging station distribution. However, the authors of [25], [26], [27] didn't present a method for providing charging services through cooperation by sharing information between charging stations.

Some studies [28], [29], [30] have been conducted on the cooperative charging scheduling model, in which discharging agents collaborate. Saner et al. [28] suggested a hierarchical multi-agent system for EV charging schedules. Low-level agents collect EV charging requests and schedule charges on account of the possible charging provision amount of CS. However, if the agent is manipulated by malicious attackers, the operation of the system may be compromised. Silva et al. [29] proposed a multi-agent selfish collaborative architecture to reduce grid overload. To decrease energy expenditures, EVs make charging decisions based on multi-agent reinforcement learning. Ding et al. [30] proposed a coordinated operation schedule that takes into account traffic conditions, renewable energy output, and charging costs. EV travel routes and charging costs are defined based on coordination optimization formulations. In [28], [29], [30], the authors studied a charging scheduling technique in which grid, CS, and EV collaborate to reduce charging peak load. However, when EVs flock without considering charging efficiency, CSs may want to monopolize the charging service and may not want to participate in a cooperation model. Therefore, a strategy that may effectively stimulate CS's participation is essential.

B. Blockchain on EV Charging Management

Kang et al. [31] proposed a P2P Electricity Trading system with CONsortium blockchain (PETCON). It uses an iterative double auction game theory for energy pricing and trading. Wang et al. [32] outlined a secure energy delivery framework in vehicular energy networks, which is based on permissioned blockchain technology. In addition, they devised a pricing-based incentive mechanism that can optimally schedule EVs' charging/discharging behaviors. Wang et al. [15] proposed a private charging pile-sharing model using coalition-matching game. Private charging pile owners and EVs are transparently matched through the blockchain. Li et al. [20] proposed a charging record management model using multi blockchain. To reduce the operation cost of the consensus process, the authors designed a distributed auction-based algorithm for optimal storage selection. In [15], [20], [31], [32], the authors proposed a blockchain-based EV charging model for efficient energy trading. However, those models did not ensure the reliability of the charging record stored in the blockchains. Malicious participants may send false charging information to the blockchain network. It has the potential to perplex participants' charging decisions.

Baza et al. [33] proposed a blockchain-assisted charging coordination mechanism so that the Energy Storage Units (ESUs) can get their charging demands in a transparent, reliable, and

TABLE I
COMPARISON OF RELATED WORK OF BLOCKCHAIN-BASED EV ENERGY TRADING MODEL

No.	Application	Motivation	Proposed model	Reliability and credibility of transactions	Motivation to participate
[31]	P2P energy trading	privacy protection and transaction security	a localized P2P Electricity Trading system with CONsortium blockchain (PETCON)	No	No
[32]	Energy delivery	potential security vulnerability in vehicular energy network and regional energy balance	blockchain-based secure incentive scheme for energy delivery	No	Yes(EVs)
[15]	Private Charging Pile (PCP) sharing	need to consider competition, cooperation and social features of EV users and PCP owners	energy blockchain-based secure PCP sharing scheme	No	No
[33]	Charging coordination between energy storage units	need for cooperation of energy storage units	blockchain-based charging coordination mechanism	No	No
[34]	Charging station selection	privacy prevention of EVs in charging bidding	privacy-preserving dynamic tariff decision protocol for electric vehicle charging	No	No
[16]	Energy trading for CS2V, V2V	prevention of denial of service (DoS) attack in energy trading and privacy prevention of EVs	privacy-preserving CS2V scheme and V2V energy trading scheme	No	No
[17]	Authentication for V2G	lack of integrity mutual authentication, identity privacy-preservation	an effective blockchain-based system model for secure and anonymous energy trading	No	No
[18]	Charging station selection	untrusted centralized nature of energy markets, identity privacy-preservation	blockchain-based secure charging station selection protocol	No	No
[19]	Charging right trading among charging stations	overload of power system	blockchain-based charging right trading model among charging stations	No	No
[20]	Charging record management	cost-efficient multi blockchain-based charging record storage operation	blockchain-based charging record management and storage selection model	No	No
Ours	Charging information sharing charging cooperation	lack of reliability of charging information and cooperation between EVSP	blockchain-based electric vehicle charging cooperation model	Yes	Yes

decentralized manner from utility companies. Moreover, the authors introduced the smart contract so that the scripts within it can schedule charging requests in a decentralized manner. To address the EV privacy issue, Knirsch et al. [34] proposed a reliable and privacy-preserving charging station selection protocol. EVs can use blockchains to find the best CS based on their location and the charging station's suggested prices. The identifier of EVs can be changed with each bidding request to protect their privacy. Danish et al. [18] proposed a smart contract-based BlockEV protocol for optimal charging station selection. In the BlockEV protocol. EVs evaluate the reputation of CSs to encourage honest CSs work. Before an EV selects a CS, it refrains from sharing any personal information with RoadSide Units (RSUs) or CSs and employs public keys as pseudonyms to preserve privacy. Ruijiu et al. [19] suggested a blockchain-based charging right trading model among EV charging stations to reduce the overload of power transmission. Each CS submits its charging demand, and a smart contract calculates charge demand satisfaction and allocates charging rights to the charging stations. CSs can trade their charging rights considering urgent charging requests. The authors of [18], [33], [34] and [19] proposed solutions for charging cooperation, but they did not consider the motivation for EVSP's participation in energy trading. Some EVSPs may not perceive the necessity of sharing charging information. If EVSP and CS are not motivated to participate in the model, it is difficult to operate a realistic model.

Table I shows the comparison of blockchain-based EV energy trading models. Existing studies have proposed models for efficient charging service provision and safe charging transactions. Nevertheless, they did not consider the reliability and credibility of charging station information. Applying blockchain technology prevents tampering and securely shares charging station information. However, since blockchain data is immutable, verifying the reliability of charging station information before recording is crucial. Additionally, it is essential to motivate different EVSPs, with varying interests, to agree to share their charging station information. The authors of [32] used incentives to encourage the participation of EVs but did not propose a method to drive the participation of EVSPs. Therefore, we propose a blockchain-based EV charging cooperation model that facilitates the sharing of trustworthy charging station information and motivates the participation of EVSPs. To establish an effective charging cooperation model, it is essential to have a short matching latency and minimize transaction overhead. To demonstrate the efficiency of our model, we selected previous EV charging matching studies [18, 34] from related studies and implemented the chaincode of these studies to evaluate the performance of these works. The evaluation results showed that our model has lower transaction overhead and charging latency compared to previous studies [18, 34]. (See Section VI-B.)

C. Shapley Value-Based Incentive Mechanism

Shapley value [22] is a solution for fairly distributing the incentive and payoff for the coalition's involved parties. Considering all possible combinations, it assigns each player an average marginal contribution. The use of Shapley value to design incentive mechanisms has been widely studied. Pilling et al. [35] adopted the cooperative game theoretic solution concept of Shapley value to fairly compensate for energy exchange between the micro grid and utility grids. Richard et al. [36] explored the cooperative settlement of internet service providers by using the Shapley value. He et al. [37] proposed a profit-sharing incentive mechanism based on the Shapley value to encourage cooperation among self-interested service providers in edge computing. The novel achievements of our work are the optimized Shapley value solution for distributing revenue fairly among multiple EVSPs and facilitating cooperation among them. The overall CS contribution value is determined based on each CS's charging activities to motivate each CS's participation.

III. BLOCKCHAIN-BASED INTEGRATED EV CHARGING PLATFORM

In this section, we define participants and possible attack models of the proposed blockchain-based integrated EV charging platform. Then we present the constituent blockchains for our platform in detail.

A. Overall Model

In our blockchain-based integrated EV charging platform, there are multiple participants: Electric Vehicles (EVs), Electric Vehicle Service Providers (EVSPs), Charging Stations (CSs), Mobile Charging Stations (MCSs), and verifier groups. Each EVSP shares its charging infrastructure, such as CS and MCS, to provide efficient charging service. EVs that register with one of the participating EVSP's charging services can use any other EVSP's charging infrastructure. Each CS's charging traffic volume information is shared in the charging traffic volume blockchain network. Our model encourages each EVSP and CS to participate in the platform by distributing rewards according to their contribution in the charging cooperation blockchain. As the contribution of each CS is determined according to the CS's activity recorded in the charging traffic volume blockchain, our model consists of the hierarchical structure consisting of a charging traffic volume blockchain and a charging cooperation blockchain. The detailed description of the participants and the constituent blockchain is as below.

1) Participants: The main participants are EVSPs, CSs, MCSs, EVs, RSUs, and the verifier group.

a) *Electric Vehicle Service Provider (EVSP):* EVSPs oversee the operation of their affiliated CSs for charging services and manage the charging infrastructure. They also offer additional services like EV charging fee payment, membership management, and incentives through the proposed platform. CS revenue is tied directly to EVSP revenue, and we assume all platform participants share the public keys of participating EVSPs.

b) *Charging Station (CS):* CSs perform charging service under specific EVSPs for EVs in a fixed location. We assume that CSs operate MCSs that can move to provide electric charging to distant EVs. CSs serve as mining and consensus nodes for the charging traffic volume blockchain and the charging cooperation blockchain. Each CS becomes the leader of the verifier group and helps EVs participate in the verifier group.

c) *Mobile Charging Station (MCS):* MCS is a mobile charging station owned and managed by a specific CS. With a smaller battery capacity than CSs, it can move to busy locations and assist with charging, reducing EV charging queues. If a driver requests emergency charging, MCSs can move a certain distance to provide charging service.

d) *Electric Vehicle (EV):* EV uses a charging service through CS or MCS. It can get charging traffic information through the charging traffic volume blockchain and select a proper CS. EV can participate in the verifier group if desired. The EV can receive incentives from the EVSP if it participates in verifying transactions. The EV should use a one-time public key to protect the EV's privacy whenever it joins the verifier group.

e) *RoadSide Unit (RSU):* RSUs, which are strategically located across geographic areas, maintain ledgers in charging traffic volume blockchains and serve as verifiers. They assist in matching nearby EVs needing charging with MCS. RSUs are always assumed to act trusted, as they operate under the government sector. We assume all participants know the locations of the RSUs.

f) *Verifier group:* A verifier group shares the charging traffic information as a transaction and verifies whether the information stored in the shared transaction matches the actual situation. Verifier group members can be divided into fixed verifiers and dynamic verifiers. A fixed verifier is a participant who becomes a member of the verifier group on a fixed basis, such as the CS and the RSU located around the CS. EVs and MCSs can act as dynamic verifiers, freely joining or leaving the verifier group.

2) Blockchains: The proposed model consists of a charging traffic volume blockchain and a charging cooperation blockchain.

a) *Charging traffic volume blockchain:* It is a private blockchain for sharing CSs' charging station information between participants. The blockchain ledger stores MCSs' public keys list, a verifier group member list, reports for each CS's charging traffic volume and charging requests. All participants can read the ledger of the charging traffic volume blockchain. However, only verifier group members enable to create transactions for reporting the charging staiton information.

b) *Charging cooperation blockchain:* It is a consortium blockchain to store the updated CS's contribution value, reward distribution results, and transactions generated between EVSPs, CSs, and MCSs. EVSPs and CSs maintain the blockchain ledger. CSs also has a role as mining nodes. The contents of the charging cooperation blockchain are not disclosed to EVs since the transactions are related to EVSP's business information. According to the CS's charging traffic information recorded in the charging traffic volume blockchain, the contribution values of each CS are updated weekly. In proportion to the contribution of the CS, the CS's vote has a weight proportional to the contribution when determining the new block using PBFT algorithm. We utilized PBFT, a widely used consensus algorithm in private blockchains, as the consensus algorithm for our private blockchain. It has low transaction latency, cost efficiency, and instant finality of transactions.

B. Adversarial Model

The proposed model focuses on achieving secure charging information sharing and motivating CS participation. We categorize adversarial attackers into three types: malicious verifiers, malicious MCSs, and greedy CSs in our proposed model. A malicious verifier attempts to spread false information to control traffic around a specific CS. It also impedes honest verifiers' participation by decreasing their trust score. When performing transaction verification, it can submit incorrect verification results to disturb the verification process. A malicious MCS, not registered in the proposed platform, can intercept trading between an honest MCS and an EV to sell its electricity to the EV. To get more incentives, a greedy CS wants to exaggerate the work recorded in the charging traffic volume blockchain. We assume that attackers can join a verifier group as a verifier and report charging information. They know a key generation protocol and can generate a public key-private key pair. Following PBFT's assumption [38], the number of adversaries does not exceed

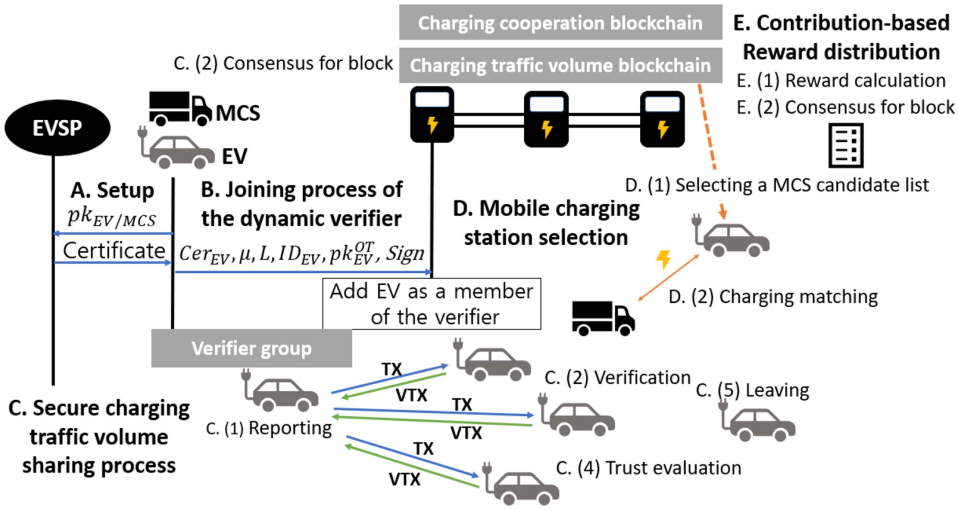

Fig. 2. The overall proposed protocol.

$\left\lfloor \frac{f-1}{3} \right\rfloor$ when the total number of participants is f. We consider the following five attacks in the proposed model.

- *False information propagation:* A malicious verifier can attempt to propagate a transaction with false charging information. It spreads false information, which conflicts with the current charging state, preventing other EVs or CSs from collecting correct information.
- *Tampering transactions:* A greedy CS tries to tamper with the charge amount and charge count recorded in the transaction before block generation. For example, when a verifier broadcasts a transaction reporting its charging amount, the CS might attempt to change the value to a larger amount to have a higher contribution value.
- *Impersonation attack:* A malicious MCS pretends to be an MCS registered in a specific CS. It can attempt to provide a charging service to EVs, interfering with other MCS's recharge transactions.
- *Disturbing transaction verification of verifier group:* A malicious verifier can transmits the verification result opposite the actual result to another verifier so that transactions with correct information are not included in the blockchain. It also may attempt to induce a delay in the verification time by not actively participating in the verification activity.
- *Collusion attack in the verifiers' trust evaluation:* A malicious verifier may intentionally give other honest verifiers a low trust score to lower the reputation of other honest verifiers. For an effective attack, malicious verifiers can collude and submit low evaluation scores when evaluating the trust values of the targeted verifiers.

IV. Proposed Protocol

In this section, we describe the protocols for the proposed EV charging system in detail. They are composed of setup, verifier group formation, secure charging traffic volume sharing process, mobile charging station selection, contribution-based reward distribution, and consensus for blocks in the charging cooperation blockchain. Fig. 2 describes the proposed protocol. The main notations are defined in Table II.

TABLE II
List of Notations

Symbol	Description
$\mathbf{EV_i}$	Electric Vehicle i
$\mathbf{CS_j}$	Charging Station j
$\mathbf{EVSP_k}$	Electric Vehicle Service Provider k
$\mathbf{MCS_m}$	Mobile Charging Station m
$\mathbf{RSU_r}$	RoadSide Unit r
$\mathbf{N}$	The size of verifier group
$\mathbf{V_n}$	Verifier group member n
pk_i	Public key of node i
sk_i	Private key of node i
pk_i^{OT}	One-time public key of mode i
sk_i^{OT}	One-time private key of node i
ID_i	Identifier of node i
$Sig_{sk_i}(M)$	ECDSA signing algorithm with sk_i for message M
q	A primer number
P	Point generator of an additive cyclic group $\mathbb{G}_q$
L	Location information
$H()$	Cryptographic hash function (eg. Keccak 256, SHA 256)
θ	Threshold value for trust evaluation
μ	Timestamp
$T_{\alpha\beta}$	Aggregated $\mathbf{V}_\beta$'s trust value, which is computed by $\mathbf{V}_\alpha$
$t_{\alpha\beta}^d$	$\mathbf{V}_\beta$'s trust score determined by $\mathbf{V}_\alpha$, , at time d
$t_{\alpha\beta}^0$	$\mathbf{V}_\beta$'s trust score determined by V_α, at the end of the last session
$\Phi_{\alpha\beta}^d$	Weight of $t_{\alpha\beta}^0$, which is used for calculating $t_{\alpha\beta}^d$ after time d of no interaction between $\mathbf{V}_\alpha$ and $\mathbf{V}_\beta$
$B_{\alpha\beta\leftarrow\tau}$	The rate at which $\mathbf{V}_\alpha$ accepts a review on $\mathbf{V}_\beta$, made by $\mathbf{V}_\tau$
$D_{\alpha\beta}$	$\mathbf{V}_\alpha$'s direct assessment score of $\mathbf{V}_\beta$
Γ	The minimum number of interactions required for trust equilibrium
λ	a decay constant of partial trust score
$Z_{\alpha\beta}$	The number of interaction between $\mathbf{V}_\alpha$ and $\mathbf{V}_\beta$
$p_{\alpha\beta}$	The proportion of a previous trust score $t_{\alpha\beta}^0$ after Z interaction

A. Setup

In this phase, each EV signs up for charging service membership and generates a public key and a private key pair through a EVSP. When a new MCS joins the platform, it needs to register with a CS. The public key of the MCS is shared by all the

participants. We assume that a public key pair of each EVSP, CS, and RSU is generated in advance, and the public keys are open to platform participants. Our protocol uses ECDSA [39], which is a digital signature algorithm used in Ethereum [40], for signature generation and verification.

EV registration:

1) $\mathbf{EV_i}$ chooses a uniformly distributed random value $sk_{\mathbf{EV_i}} \in \mathbb{Z}_q$ as a private key and computes a public key $pk_{\mathbf{EV_i}} = sk_{\mathbf{EV_i}}P$. The P is a point generator of an additive cycle group of a selected elliptic curve over a finite field. The $\mathbf{EV_i}$ submits the $pk_{\mathbf{EV_i}}$ to $\mathbf{E_k}$.
2) The $\mathbf{EVSP_k}$ issues a certificate for $pk_{\mathbf{EV_i}}$ to the $\mathbf{EV_i}$. The $\mathbf{EVSP_k}$'s signature for the $pk_{\mathbf{EV_i}}$ is included in the certificate.
3) The $\mathbf{EVSP_k}$ registers the $\mathbf{EV_i}$ as a charging service member. We assume that $ID_{\mathbf{EV_i}} = H(pk_{\mathbf{EV_i}})$ is used as an identifier of $\mathbf{EV_i}$.

MCS registration:

1) $\mathbf{MCS_m}$ randomly selects a private key $sk_{\mathbf{MCS_m}} \in \mathbb{Z}_q$, and computes a public key $pk_{\mathbf{MCS_m}} = sk_{\mathbf{MCS_m}}P$. It sends the $pk_{\mathbf{MCS_m}}$ to a $\mathbf{CS_j}$.
2) The $\mathbf{CS_j}$ adds the public key of the $\mathbf{MCS_m}$ to its MCS public key list.
3) The $\mathbf{CS_j}$ shares the updated public key list of MCSs in the charging traffic volume blockchain.

B. Joining Process of the Dynamic Verifier

In this phase, dynamic verifiers, such as EV and MCS, join in the verifier group.

Joining process:

1) $\mathbf{EV_i}$ chooses a randomly distributed secret value $sk^{OT}_{\mathbf{EV_i}}$. It calculates $pk^{OT}_{\mathbf{EV_i}} = sk^{OT}_{\mathbf{EV_i}}P$ to participate in the verifier group where a $\mathbf{CS_j}$ is the leader. It generates a self-signed certificate $\{\upsilon, \eta\}$ by signing $pk^{OT}_{\mathbf{EV_i}}$ with its private key $sk_{\mathbf{EV_i}}$. The self-signed certificate proves that the $pk^{OT}_{\mathbf{EV_i}}$ is generated by the $\mathbf{EV_i}$. The generation process of the self-signed certificate is as follows.
   - The $\mathbf{EV_i}$ chooses a uniformly distributed random value ι between a range [1,q-1].
   - The $\mathbf{EV_i}$ calculates a $\upsilon = \iota P$ and a $\eta = (H(pk^{OT}_{\mathbf{EV_i}}||\mu) + sk_{\mathbf{EV_i}}\upsilon)\iota^{-1}(modq)$.
   - The (υ, η) is used as a self-signed certificate for the $pk^{OT}_{\mathbf{EV_i}}$.
2) The $\mathbf{EV_i}$ submits $\{Cer_{\mathbf{EV_i}}, \mu, L, ID_{\mathbf{EV_i}}, pk^{OT}_{\mathbf{EV_i}}, Sig_{sk_{\mathbf{EV_i}}}(\mu||L||ID_{\mathbf{EV_i}}||pk^{OT}_{\mathbf{EV_i}})\}$ to the $\mathbf{CS_j}$. The $Cer_{\mathbf{EV_i}}$ is $\mathbf{EV_i}$'s self-signed certificate. If a $\mathbf{MCS_m}$ joins the verifier group, the $\mathbf{MCS_m}$ submits $\{\mu, L, ID_{\mathbf{MCS_m}}, Sig_{sk_{\mathbf{MCS_m}}}(\mu||L||ID_{\mathbf{MCS_m}})\}$ to the $\mathbf{CS_j}$.
3) The $\mathbf{CS_j}$ checks if the $\mathbf{EV_i}$ or the $\mathbf{MCS_m}$ is located around it and verifies the submitted signature value.
4) The $\mathbf{CS_j}$ adds the $\mathbf{EV_i}$ or the $\mathbf{MCS_m}$ as a member of the verifier group and shares the updated public key list of the verifier group members through the blockchain. The $\mathbf{EV_i}$ or the $\mathbf{MCS_m}$ participates in the blockchain network as client nodes and receives the current blockchain ledger from other blockchain nodes. The $\mathbf{EV_i}$ uses $pk^{OT}_{\mathbf{EV_i}}$ as its one-time public key, and the hash value of the public key is used as its one-time identifier $ID^{OT}_{\mathbf{EV_i}}$. To preserve the EV's privacy, it generates a new one-time public key pair whenever it participates in another verifier group. Verifiers receive incentives based on the number of transactions they verify and their trust score from EVSP.

C. Secure Charging Traffic Volume Sharing Process

Verifier group members share the CS's charging information by broadcasting a transaction. The verifier group member verifies the reliability of the transaction contents. According to the verification result, the CS creates a block and agrees on the block with other CSs by using RAFT (Reliable, Replicated, Redundant, And Fault-Tolerant) [41], which is efficient in the Internet Of Things (IoT) environments and well-suited for private blockchains. Verifier group members evaluate the trust value of other members through verification experience. The detailed process is as follows.

Reporting charging information:

1) $\mathbf{V_n}$ generates a transaction for reporting $\mathbf{CS_j}$'s charging information. The components of a traffic volume transaction TX are shown below.

$$TX = \{D, \mu, ID_{\mathbf{CS_j}}, ID_{\mathbf{V_n}}, report, Sig_{sk_{\mathbf{V_n}}}(D||\mu||ID_{\mathbf{CS_j}}||report)\} \quad (1)$$

   The $report$ means charging information of $\mathbf{CS_j}$, each MCS's charging state and charging requests for MCS. It could include charging amount, charging time, and charger type. The D is date information and $ID_{\mathbf{V_n}}$ is the identifier of the reporting verifier group member. When a $\mathbf{EV_i}$ reports the transaction, it uses $ID^{OT}_{\mathbf{EV_i}}$ as $ID_{\mathbf{V_n}}$.
2) The $\mathbf{V_n}$ propagates the transaction TX to the surrounding verifier group members. The TX is added to the transaction pool in the verifier group and is shared by all.

Verification:

1) When other verifier group members $\mathbf{V_x}(\mathbf{x} \neq \mathbf{n}, \mathbf{x} = 1, \ldots, \mathbf{N})$ receive a $\mathbf{V_n}$'s transaction, they verify the signature and check whether the $\mathbf{V_n}$ is the verifier group member or not. Moreover, they check whether the transaction report matches the current CS status and other verifier's transaction contents. If they agree to the content, each $\mathbf{V_x}$ creates a signature for the transaction and generates a verification message VTX as follows.

$$VTX = \{TX, \mu, ID_{\mathbf{V_x}}, Sig_{sk_{\mathbf{V_x}}}(TX||\mu||ID_{\mathbf{V_x}})\} \quad (2)$$

2) The VTX of the $\mathbf{V_x}$ is shared to all the verifier group members through the transaction pool.
3) If the number of the VTX for TX is more than $\frac{2}{3}$ of the total number of verifier group members, a $\mathbf{CS_j}$ and the verifier group members broadcasts the VTX to other CSs and EVs.

Consensus for the charging traffic volume blockchain:

1) An election process of RAFT consensus chooses one charging station as a leader for a given term. Other charging stations become followers, which will accept the leader's decision.
2) When the leader receives transactions from the verifier group, it begins the log replication process by sending Append Entries RPCs containing the latest transaction entries to followers.

Algorithm 1: Trust Value Evaluation.

Input: $t^d_{\tau\beta}, D_{\alpha\beta}$, the number of verifiers s
if $d == Z_{\alpha\beta} == 0$ **then**
  $T_{\alpha\beta} = t^0_{\tau\beta} = 0.5$
end
$\Phi^d_{\alpha\beta} \leftarrow e^{\lambda_{\alpha\beta} d}$
$B_{\alpha\beta\leftarrow\tau} \leftarrow (1 - |\frac{t^d_{\tau\beta} - t^0_{\alpha\beta}}{t^0_{\alpha\beta}}|) \times (1 - \Phi_{\alpha\tau}) \times t^d_{\alpha\tau}$
$p_{\alpha\beta} \leftarrow max((1 - \frac{Z_{\alpha\beta}}{\Gamma}) \times \Phi^d_{\alpha\beta}, 0)$
if $Z_{\alpha\beta} == 0$ **then**
  $T^d_{\alpha\beta} \leftarrow \frac{D_{\alpha\beta} + (\Phi^d_{\alpha\beta} \times t^0_{\alpha\beta}) + \sum_{\tau=1}^{s-1} B_{\alpha\beta\leftarrow\tau} \times t^d_{\tau\beta}(p_x)}{1 + \Phi^d_{\alpha\beta} + \sum_{\tau=1}^{s-1} B_{\alpha\beta\leftarrow\tau}}$
else
  if $Z_{\alpha\beta} > 0$ **then**
    $T^d_{\alpha\beta} \leftarrow \frac{D_{\alpha\beta} + (p_{\alpha\beta} \times t^0_{\alpha\beta})}{1 + p_{\alpha\beta}}$
  end
end

3) Followers append the new transactions to their logs and send a confirmation message to the leader CS.
4) After receiving confirmation messages from a majority of followers, the leader CS commits the entries to its own log. The leader then notifies followers of the committed entries, ensuring that they also commit them to their logs, thereby achieving consensus.
5) Each CS propagates the updated blockchain ledger to all other platform participants.

Trust evaluation:

1) Each verifier group member $\mathbf{V}_\alpha$ broadcasts $t^d_{\alpha\beta}$, which is a $\mathbf{V}_\beta$'s trust score evaluated by the $\mathbf{V}_\alpha$ at time d, to other verifier group members. Each $\mathbf{V}_\alpha$ determines a $t^d_{\alpha\beta}$ based on the $\mathbf{V}_\beta$'s verification activities and trust score rating pattern.
2) Each verifier group member $\mathbf{V}_\alpha$ collects a trust value $t^d_{\tau\beta}$ of verifier member $\mathbf{V}_\beta$ from the other member $\mathbf{V}_\tau$,
3) Based on the $t^d_{\tau\beta}$, the $\mathbf{V}_\alpha$ calculates the trust value $T_{\alpha\beta}$ of other $\mathbf{V}_\beta$ using CTRUST model [42]. Considering the environment where multiple EVs dynamically participate in verification groups and trust values need to be determined by incorporating the opinions of nearby verifiers, CTRUST has been chosen as the trust model. The calculation process is shown in Algorithm 1. An initial trust value $t^d_{\alpha\beta}$ and an initial aggregated trust value $T_{\alpha\beta}$ are set to 0.5. A $t^d_{\alpha\tau}$ decreases as time passes by weighting $\Phi^d_{\alpha\beta}$ for time degradation of the trust value. As $t^0_{\alpha\beta}$ becomes similar to the $t^d_{\tau\beta}$, the weight of $t^d_{\tau\beta}$ in calculating the aggregated $T_{\alpha\beta}$. Additionally, when the interaction between $\mathbf{V}_\alpha$ and $\mathbf{V}_\beta$ increases, the $T_{\alpha\beta}$ reaches a specific value.
4) If the calculated $T_{\alpha\beta}$ is θ or less, the $\mathbf{V}_\alpha$ notifies it through the charging traffic volume blockchain. When the majority of verifier group members report that the $\mathbf{V}_\beta$'s trust value is less than θ, the members determine that $\mathbf{V}_\beta$ is malicious. The $\mathbf{CS_j}$ prevents the $\mathbf{V}_\beta$ from participating in the verifier group anymore.

Leaving process of a dynamic verifier:

1) A leaving $\mathbf{V}_n$ submits a request message to $\mathbf{CS_j}$ to get incentives as below. The request message includes $\mathbf{V_n}$'s activity history and $\mathbf{V_n}$'s signature.

$$\left\{List^{\mathbf{V_n}}_{VTX}, \mu, ID_{\mathbf{V_n}}, Sign_{sk_{\mathbf{V_n}}}(List^{\mathbf{V_n}}_{VTX} || \mu || ID_{\mathbf{V_n}})\right\} \tag{3}$$

The $List^{V_n}_{VTX}$ is the list of VTXs generated by the $\mathbf{V_n}$.
2) The $\mathbf{CS_j}$ checks the request message and incentives the $\mathbf{V_n}$ proportionally to the VTX it has created. Incentive payments are carried out in the off-chain network.
3) The $\mathbf{CS_j}$ deletes the $\mathbf{V_n}$'s public key from its verifier group member list and shares the updated list through the charging traffic volume blockchain network.

D. Mobile Charging Station Selection

When an EV faces difficulty reaching CSs, it can submit a charging request to MCS in the charging traffic volume blockchain. The EV selects its desired MCS based on the shared MCS state. The EV broadcasts a charging request transaction to the blockchain. If the EV is not a verifier member, it disseminates the transaction through nearby RSUs. The MCS, which the EV wishes to charge from, responds with an acceptance transaction, and the RSU facilitates the matchmaking process between the MCS and the EV.

Selecting a MCS candidate list:

1) Each $\mathbf{MCS_m}$ periodically broadcasts a TX in the charging traffic volume blockchain. The $report$ of the TX is shown below.

$$\{ID_{\mathbf{MCS_m}}, STATE_m, COST_m, E^{am}_m, L\} \tag{4}$$

A $STATE_m$ refers to the current status of the $\mathbf{MCS_m}$, which can be one of the following: {charging, moving, idle}. A $COST_m$ is a charging cost per unit charge, and a E^{am}_m is a possible charging amount of $\mathbf{MCS_m}$.
2) The $\mathbf{EV_i}$ selects an MCS, which locates within a specific distance, has a acceptable charging cost, and has enough charging amount as shown in (5).

$$\begin{aligned} d(\mathbf{MCS_m}, \mathbf{EV_i}) &\le th_{dis} \\ COST_m * E^{req}_i + callfee_m &\le th_{cost} \\ E^{am}_m &\ge E^{req}_i \end{aligned} \tag{5}$$

The function $d()$ provides the distance between two inputs. The th_{dis}, th_{cost}, and E^{req}_i represent the maximum allowable distance between the $\mathbf{EV_i}$ and $\mathbf{MCS_m}$, $\mathbf{EV_i}$'s desired charging cost, and the required charging amount, respectively. The $callfee_m$ signifies the cost associated with summoning $\mathbf{MCS_m}$.

Charging matching:

1) The $\mathbf{EV_i}$ submits the TX containing $report$ information to a nearby $\mathbf{RSU_r}$ to request charging. If the $\mathbf{EV_i}$ selects $\mathbf{MCS_1}$, $\mathbf{MCS_2}$, and $\mathbf{MCS_3}$ as candidates, The $report$ is structured as follows:

$$\left\{ID_{\mathbf{MCS_1}}, ID_{\mathbf{MCS_2}}, ID_{\mathbf{MCS_3}}, ID_{\mathbf{RSU_r}}, E^{/req}_i, T\right\} \tag{6}$$

To prevent the exact location of the $\mathbf{EV_i}$ from being exposed, the RSU_r information is included in the $report$ instead of $\mathbf{EV_i}$'s location information.

TABLE III
VALUE FUNCTIONS

No	value function	Description
1	s1	Total number of EV charged by a coalition G for a week
2	s2	Total charging amount of a coalition G for a week
3	s3	Total number of charge of a coalition G through MCS for a week
4	s4	Total charging amount of a coalition G through MCS for a week

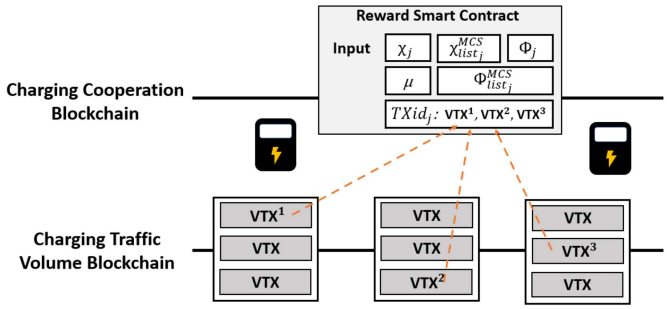

Fig. 3. Transactions of the proposed platform.

2) The $\mathbf{RSU_r}$ distributes the TX received from the EV_i to the charging traffic volume blockchain. One of the candidate MCS confirms the match by deploying an acceptance transaction. The matched MCS can request the precise location of the $\mathbf{EV_i}$ from the $\mathbf{RSU_r}$.

E. Contribution-Based Reward Distribution

A reward smart contract calculates each CS's contribution value based on the charging history of CSs in the charging traffic volume blockchain. The contract is deployed in the charging cooperation blockchain in advance. Fig. 3 shows an example of transactions of the proposed platform. We assume that the contribution value is updated every week.

Reward calculation:

1) Each $\mathbf{CS_j}$ submits input values to execute a reward smart contract for Shapley value calculation. Detection of incorrect values is possible as input values are linked to blockchain transactions of charging traffic volume. The input value is shown below.

$$\left\{\chi_j, \chi_{list_j}^{MCS}, \phi_j, \phi_{list_j}^{MCS}, \mu, TXid_j\right\} \tag{7}$$

The χ_j denotes the total number of EV charged by $\mathbf{CS_j}$, and the $\chi_{list_j}^{MCS}$ is a list of the number of charges provided by $\mathbf{CS_j}$. The ϕ_j and $\phi_{list_j}^{MCS}$ are the total charging amount of $\mathbf{CS_j}$, and the total charging amount of $\mathbf{CS_j}$'s MCSs that supported other CSs for a week, respectively. The $TXid_j$ denotes the list of an identifier of transactions recorded in the charging traffic volume blockchain, which proves a $\mathbf{CS_j}$'s charging activities.

2) The reward smart contract calculates the Shapley value of $\mathbf{CS_j}$ for each contribution factor based on the input value. Let I be a set that collects all the participating CS. A coalition G is a subset of I. The $s_1(G), s_2(G), s_3(G)$, and $s_4(G)$ denote the value functions to compute the marginal contribution value. The definition of the value functions is described in Table III.

3) The Shapley value $\varphi_{cf}(I, \mathbf{CS_j})$ of each CS is automatically calculated by the following formula in a reward smart contract of charging cooperation blockchain. The (8) calculates $\mathbf{CS_j}$'s marginal contribution value of overall charging cooperation.

$$\varphi_{cf}(I, \mathbf{CS_j}) = \sum_{G \subseteq \omega : \mathbf{CS_j} \notin G} \frac{|G|!(I - |G| - 1)!}{\omega!} (s_{cf}(G \cup \mathbf{CS_j}) - s_{cf}(G)) \tag{8}$$

4) Based on the Shapley value, the contribution value C_j of each $\mathbf{CS_j}$ is determined in the smart contract as below. The W_1, W_2, W_3 and W_4 are weight values for each contribution factor $(W_1 + W_2 + W_3 + W_4 = 1)$. For each contribution factor, the final contribution value of a charging station (CS) is calculated by determining the proportion of the $\mathbf{CS_j}$'s contribution value to the total contribution value sum of all CSs. This proportion is then multiplied by the weight and applied to determine the $\mathbf{CS_j}$'s final contribution value.

$$C_j = W_1 \frac{\varphi_1(I, \mathbf{CS_j})}{\sum_{J=1}^{\omega} \varphi_1(I, \mathbf{CS_J})} + W_2 \frac{\varphi_2(I, \mathbf{CS_j})}{\sum_{J=1}^{\omega} \varphi_2(I, \mathbf{CS_J})} + W_3 \frac{\varphi_3(I, \mathbf{CS_j})}{\sum_{J=1}^{\omega} \varphi_3(I, \mathbf{CS_J})} + W_4 \frac{\varphi_4(I, \mathbf{CS_j})}{\sum_{J=1}^{\omega} \varphi_4(I, \mathbf{CS_J})} \tag{9}$$

5) Each $\mathbf{CS_j}$ checks its C_j and sends an agreement transaction to the smart contract if it agrees with the result.

6) When two-thirds of all CS agree on the result, the smart contract calculates each CS's reward in proportion to the C and records it in the blockchain.

Consensus for the charging cooperation blockchain:

1) A CS with the highest contribution value becomes the primary node in the charging cooperation blockchain for a week. It creates a new block $Block_{co}$ by collecting the transactions propagated by other CSs.

2) The primary node propagates $\boldsymbol{Pre-prepare}$ message to all other CSs. The message is $< \boldsymbol{Pre-prepare}, Block_{co}, h(Block_{co}, \mu) >$.

3) When each CS receives the $\boldsymbol{Pre-prepare}$ message, it checks whether the signatures of the verifier group members are included in the transaction of the block, and verifies the signature value and the hash value of the block. After verification, each CS transmits $< \boldsymbol{Prepare}, Block_{co}, h(Block_{co}), \mu >$ to other CSs.

TABLE IV
PARAMETERS

Parameters	Values
λ	0.8
θ	0.45
$t^0_{\tau\beta}$	0.5
A size of the verifier group	60

4) Let's assume that a CS receives L $\boldsymbol{Prepare}$ from $\mathbf{CS_1}, \ldots, \mathbf{CS_L}$. If $\frac{\sum_{j=1}^{L} C_j}{\sum_{j=1}^{\omega} C_j} > \frac{2}{3}$ is satisfied, the CS broadcasts a $\boldsymbol{Commit}$ message to all other CSs. The $\boldsymbol{Commit}$ message is $< \boldsymbol{Commit}, Block_{co}, \mu >$.
5) Upon receiving H $\boldsymbol{Commit}$ message satisfying $\frac{\sum_{j=1}^{H} C_j}{\sum_{j=1}^{\omega} C_j} > \frac{2}{3}$, each $\mathbf{CS_j}$ adds the $Block_{co}$ to the charging cooperation volume blockchain ledger.
6) Each $\mathbf{CS_j}$ shares the updated blockchain ledger with other participants.

V. Security Analysis

In this section, we describe how the proposed model prevents false charging information propagation, transaction tampering, and impersonation attack. We also provide the simulation results to show that the proposed model can restrain the malicious activities of verifiers and the collusion attack of some malicious verifiers. We used Matlab [43] for the simulation. Table IV shows the parameter used in the simulation. According to the report [44], the worldwide average number of EVs per charger in 2021 was 10, and the average number of chargers per electric charging station in Indiana was 4. Considering these statistics and the fact that vehicles or RSUs are usually near the CS, we set the number of verifier group members to 60. We set that the trust score ranges from 0 to 1, and verifiers with scores lower than 0.5 are set as malicious.

A. Resistance Against False Charging Information Propagation

A malicious verifier reports a transaction with false information. To enable transactions to be stored on the blockchain, more than $\frac{2}{3}$ verifier members should generate VTXs for the transaction. The valid VTX includes $Sig_{sk_{\mathbf{Vg_x}}}(TX||\mu||ID_{\mathbf{Vg_x}})$, which is a signature created by other verifiers' private keys. When verifier members find that the contents of the transaction are different from the actual situation, they will not generate a VTX for the transaction. Depending on the difficulty of the mathematical problem underlying the signature algorithm used, a malicious verifier cannot forge a valid VTX. Since the transaction with false information cannot collects enough VTXs, it cannot be recorded on the blockchain. Therefore, our model prevents false charging information propagation.

B. Resistance Against Transaction Tampering

A greedy CS attempts to alter a $report$ into a $report'$ containing wrong information in a VTX. To achieve its goal, the greedy CS needs to generate $Sig_{sk_{\mathbf{Vg_n}}}(D||\mu||ID_{\mathbf{CS_j}}||report')\}$ on a forged TX' and creates $Sig_{sk_{\mathbf{Vg_x}}}(TX'||\mu||ID_{\mathbf{Vg_x}})$. However, since the CS doesn't know the private keys of the verifier group members, it can't generate a valid signature on the forged transaction. Transactions with invalid signatures will be rejected in the consensus process. Therefore, our model can prevent transaction tampering.

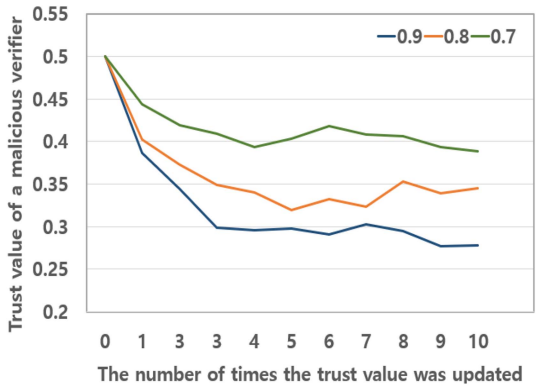

Fig. 4. Trust value evaluation of a malicious verifier.

C. Resistance Against Impersonation Attack

A malicious MCS may attempt to trick an EV by pretending to be a registered MCS. It can generate a fake identifier, or use a public key of a registered MCS for an impersonation attack. Let's assume that a malicious MCS, $\mathbf{MCS'_m}$ pretends to be an registered $\mathbf{MCS_m}$. When $\mathbf{V_i}$ meets the malicious $\mathbf{MCS'_m}$ for energy trading, the $\mathbf{V_i}$ sends $\{\mu, ID_{\mathbf{V_i}}\}$ to the $\mathbf{MCS'_m}$, and requests $\mathbf{MCS'_m}$ to generate $Sig_{sk_{\mathbf{MCS_m}}}(\mu||ID_{\mathbf{V_i}})$. As $\mathbf{MCS'_m}$ has no knowledge of $sk_{\mathbf{MCS_m}}$, it cannot create a valid $Sig_{sk_{\mathbf{MCS_m}}}(\mu||ID_{\mathbf{V_i}})$. The $\mathbf{V_i}$ can access a list of registered MCS's public keys through the charging traffic volume blockchain ledger so it can verify a signature which $\mathbf{MCS'_m}$ has sent. Since the verification will fail, $\mathbf{V_i}$ can detect that $\mathbf{MCS'_m}$ is not $\mathbf{MCS_m}$. Therefore, the proposed model is resistant against impersonation attacks from a malicious MCS.

D. Limiting Malicious Verifier's Activities

Malicious verifiers submit incorrect verification results in the verification process. In the proposed model, other verifiers will give low trust scores to these attackers when they see their malicious behaviors. We simulated the trust evaluation of a malicious verifier according to the ratio of malicious acts among the verifier's total acts. As shown in Fig. 4, when acting maliciously with 90 % probability, the average trust value of this verifier falls below 0.3 after three evaluation periods. Suppose the trust value threshold determining the verifier as a malicious node is 0.45 or higher. In all experimental scenarios, a malicious verifier is detected after the initial trust period, and if their trust value falls below the threshold, they are excluded from the verifier group. Therefore, our model could limit its activities in the verifier group. Conversely, a verifier can rebuild its trust by acting honestly in subsequent periods. Fig. 5 shows the change in the trust value of the verifier, which initially has a trust value of 0.4 from other verifiers. It indicates that the verifier's trust

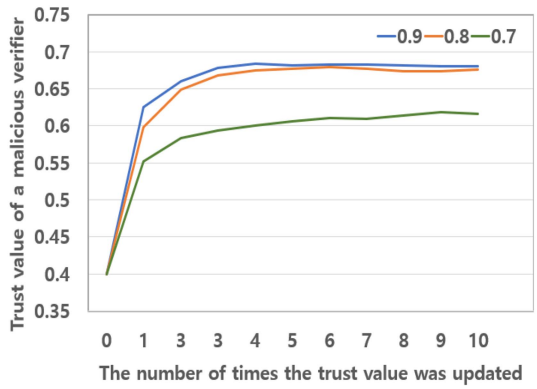

Fig. 5. Trust value evaluation of an honest verifier.

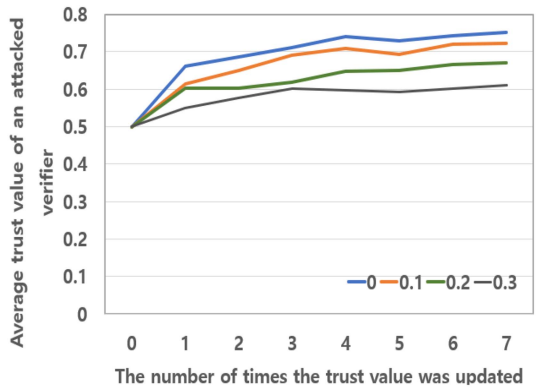

Fig. 6. Trust value evaluation of an attacked honest verifier.

value increases to 0.55 or higher after the first evaluation for every case.

E. Resistance Against Collusion Attack of Malicious Verifiers in the Trust Value Evaluation

A platoon of malicious verifiers may submit a low trust value to reduce other honest verifier's trust value to exclude it. Other verifiers will give a low trust score to these attackers when knowing the malicious behavior. We simulated the average trust score of an honest verifier when the ratio of the malicious verifier platoon was 0, 0.1, 0.2, and 0.3, respectively. According to the assumption of the proposed model, the ratio of malicious verifiers is not higher then $\frac{2}{3}$. We assume that a malicious verifier platoon submits a trust score between 0 and 0.5 randomly for an honest verifier. After the first trust evaluation, other verifiers give a trust score between 0 and 0.5 for a malicious verifier platoon since they notice the malicious behaviors. As shown in Fig. 6, when the malicious verifier platoon exists, the trust score of the attacked verifier is evaluated lower than when there is no malicious verifier platoon. However, the verifier's trust score is recovered during the trust evaluations as malicious participants are excluded. The simulation results showed that our model is resistant against to collusion attack in the trust evaluation.

TABLE V
DRIVING SCENARIO

Case	Origin	Destination	Distance (km)
1	11354 W Stones Hill Rd, Ligonier, IN 46767, US	1165 Chappelow Ridge Rd, West Harrison, IN 47060, US	555
2	409 N Co Rd 75 W, Greencastle, IN 46135, USA	55969 Tulip Rd, New Carlisle, IN 46552, USA	547
3	S 500 W, Crawfordsville, IN 47933, USA	30734 Co Rd 24, Osceola, IN 46561, USA	498
4	4996 S 75 W, La Porte, IN 46350, US	7921-7505 US-150, West Terre Haute, IN 47885, US	566

VI. SIMULATION AND PERFORMANCE EVALUATION

In this section, we evaluated the performance of the proposed model by simulating the charging cooperation of CSs. We utilized ArcGIS [45], AnyLogic [46], and Matlab [43] for the simulation. We used existing EV charging stations' data in the state of Indiana, US [47] [48] as the use case. The simulation results showed that the proposed model can reduce the charging waiting time of EVs by applying MCS. In addition, we implemented a prototype of the charging traffic volume blockchain for our model by using Hyperledger Fabric 2.2 [49]. To demonstrate the effectiveness of our model, we evaluated the performance of our charge matching protocol in comparison to the previous works [18], [34].

A. Simulation of Charging Cooperation

1) Dataset: We use the data which is the 2015 Indiana Statewide Travel Demand Model (ISTDM). ISTDM is Indiana Department Of Transportation (INDOT)'s published projection model for planning statewide projects [24]. It consists of traffic volumes and locations of origin-destination data in Indiana. We included the existing charging stations in Indiana but excluded charging stations exclusive to specific manufacturers and located further than a half mile away from Alternative Fuel Corridors (AFC). We simulated (1) EVs' long-distance trips within Indiana using the origin-destination traffic data, (2) how often they charged, and (3) how much energy they consumed to recharge during their long-distance trips. When EV charge drops below 20 % on the way, we assume that it will get charged at the nearest charging station along the current route. We obtained the number of chargers of each CS, the amount of charge provided for a day, and the number of charges through the dataset.

2) Charging Cooperation Scenario: We performed simulations for the following charging scenarios to analyze the proposed model.

a) Long distance drivers scenario: EVs can request emergency charging services from MCS via the charging traffic volume blockchain. To demonstrate that long-distance drivers can drive efficiently with MCSs, we simulated a long-distance driver's charging scenario. Four randomly selected long-distance driving routes used in the simulation are shown in Table V. When the EV's driving distance exceeds 100 km, it visits the nearest CS or MCS for charging. The total battery capacity is 65.8 kWh, which is the average battery usable [50], and the energy consumption efficiency is 199 Wh/km which is the average energy consumption of all EVs [51]. We assumed that the driver fully charged the vehicle's battery when he used a charging service. In the scenario where a MCS is applied, the CS, which is the closest to the driving route, sends a MCS to an

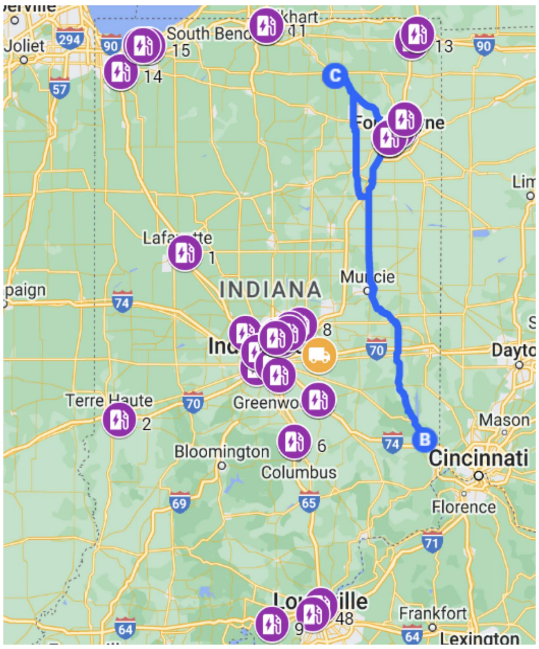

Fig. 7. A map for charging scenario in the state of Indiana, US.

TABLE VI
PARAMETERS

Parameters	Settings
velocity of MCSs	50 km/h ± 10%
Charging time	[60, 120]
The number of chargers in public charging spot	4
Maximum cooperation range	10 km
The number of charging stations	14
The number of public charging spots	10

EV requested charging. Fig. 7 illustrates the CS's location and driving route of the first long-distance driving scenario.

b) Public charging points scenario To demonstrate our charging cooperation scenario in public charging points, we chose Fort Wayne, which is a city in Indiana, for a realistic situation. CSs can support charging through MCSs in areas where charging demand is high, such as shopping centers, hospitals, and airports in Fort Wayne. We denote a place that provides charging service in a public place as a public charging point. We set that each densely populated area has a charging point with 4 EV chargers, which is the average number of chargers at charging stations in Indiana. If there are more EVs that want to charge than chargers in the charging spot, they can request nearby MCS through the blockchain. In this scenario, the CS closest to the charging point, or the second closest CS, sends MCS to the charging spot. We assume that busy CSs with many EVs use their MCSs for their EV customers. The parameter used for the charging simulation is shown in Table VI. The velocity of MCSs averages 50 km/h. The charging time of each EV is randomly selected between 60 min and 120 min. MCSs go to areas within 10 km of their location in the scenario. Fig. 8 shows the map of Fort Wayne indicating the location of CSs and the public charging spots. There are 14 charging stations and 10 public charging points on the map.

3) Simulation Results: We analyzed driving distance and charging latency through simulation of charging scenarios to demonstrate the efficiency of long-distance driving for drivers through the application of MCS.

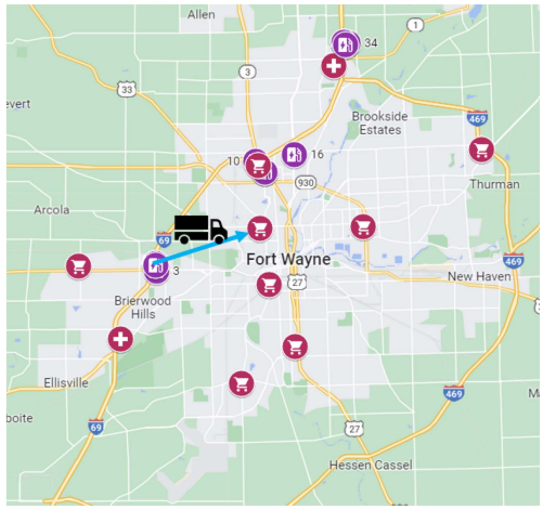

Fig. 8. A map for charging scenario in the Fort Wayne.

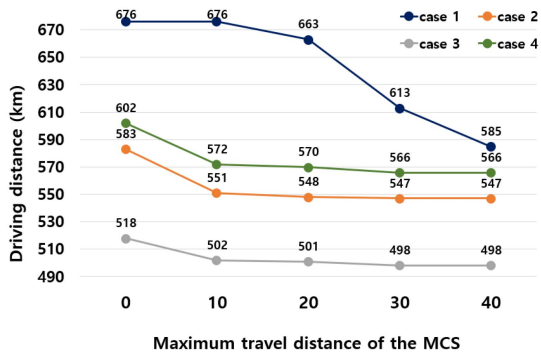

Fig. 9. EV driving distance in relation to MCS travel distance.

a) Analysis of charging efficiency for long-distance drivers using the MCS: We simulated long-distance driving charging scenarios to show that using MCSs reduces range anxiety in long-distance drivers. Fig. 9 depicts the change in total driving distance for the four long-distance driving scenarios based on an activity of the MCS's maximum moving distance. The MCS's maximum travel distance of 0 indicates that the EV directly visits the CS without using the MCS. In most cases, the total driving distance of EVs decreased with the introduction of MCS because the EV is recharged by first meeting the MCS instead of going to a more distant CS. However, Case 1 shows that moving the MCS by 10 km does not affect the total driving distance of the EV, whereas moving the MCS by 20 km decreases the EV's driving distance. It shows that the MCS needs to move more than 20 km so that the driver can benefit from the driving distance. Except for Case 1, the EV's total driving distance is the same in Cases 2, 3, and 4, where the MCS's travel distance is 30 km and 40 km, respectively. These values equal the minimum driving distance in each of the routes shown in Table V. It indicates that the MCS does not need to travel more than 30 km in Case 2, 3, and 4 routes. Case 1 demonstrates that if the MCS can travel 40 km, the EV's total driving distance will be reduced even further. The

TABLE VII
PERCENTAGES OF MINIMUM REMAINING BATTERY POWER OF THE EV IN EACH DRIVING CASE

Maximum travel distance of the MCS(km)	Case 1	Case 2	Case 3	Case 4
0	26.78%	43.49%	26.17%	18.58%
10	31.04%	45.62%	28.82%	22.23%
20	44.40%	47.62%	32.86%	23.14%
30	46.53%	50.88%	35.90%	28.30%
40	53.82%	58.68%	38.63%	31.65%

simulation results showed that MCS's charging service shortens the EV's driving distance.

Table VII compares the percentage of minimum remaining battery power based on the maximum travel distance of the MCS. If the remaining battery capacity is higher, long-distance drivers will experience less range anxiety. The longer the MCS travels, the shorter the EV travels to a charging point, reducing battery consumption. The EV in Case 4 has a minimum remaining battery capacity ratio of 18.58 % when there is no MCS. Assuming an energy consumption of 199 Wh/km, the EV can travel 61 km further. If there is no CS within 61 km, the EV will run out of battery. In Case 4, the EV has a minimum remaining battery capacity of 31.65 % when the MCS's maximum travel distance is 40 km. The use of MCS increased the minimum remaining battery charge by at least 3.17 % on average in the four long-distance driving scenarios. As a result, our model can improve long-distance drivers' driving efficiency and decrease range anxiety.

b) Analysis of EV's charging latency according to the number of MCSs: To analyze the charging waiting time, we simulated a scenario in which a CS helps charging through MCS at other busy CSs or pubic charging points. Each CS has the same number of MCS, and each public charging point has 4 chargers, as shown in Table VI. Following the global EV outlook in [52], the number of EVs per charging point in the United States and Japan are 18.2 and 11.9, respectively, which are higher than the world average. We calculated the average EV charging latency time when the number of EVs per charging point was 11 and 18. The arrival time of each EV at the charging station was randomly determined according to a Gaussian probability distribution. We assumed that EVs are charged from 10 am to 4 pm, corresponding to the charging peak hour [53]. At this time, we simulated the standard deviation values σ of 60, 120, 180, and 240.

Fig. 10 shows the change in charging waiting time according to the number of MCSs when the number of EVs per charging point is 12. If the MCSs are not applied, the average waiting time is 98.5, 90.7, 79.7, and 74.8 min, respectively, when the σ is 60, 120, 180, and 240. When each CS operates three MCSs, EVs' average charging waiting time was reduced by up to about 46.9 % compared to when MCS is not applied. The simulation result demonstrated that the application of MCSs effectively reduced the charging waiting time. As the number of MCSs operated by each CS goes up, the average EV charging waiting time gradually decreases. Since the number of EV is limited, the waiting time becomes constant when more than a certain number of MCSs is applied. As shown in Fig. 10, if the number of MCSs of each CS is 8, the latency time no longer decreases significantly. The

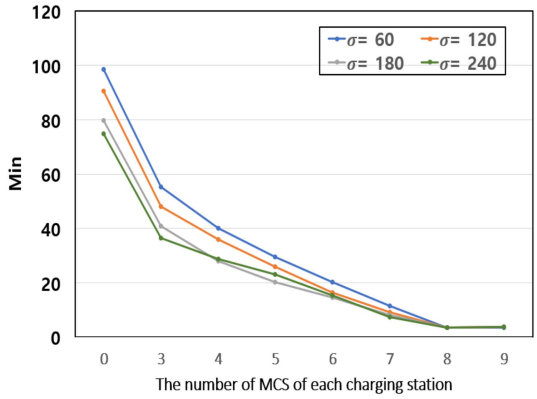

Fig. 10. Charging latency (EVs per charging point : 12).

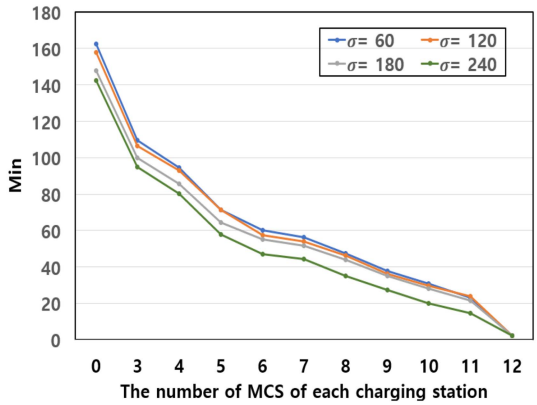

Fig. 11. Charging latency (EVs per charging point : 18).

waiting time is under 5 min for every case, which is an adequate charging standby time when each CS has 7 MCSs. Fig. 11 shows the charging latency time when the EVs per charging point is 18. At this time, the waiting time for charging increases compared to when the number of EVs per charging station is 11 because many vehicles are gathered at a more specific charging location. Unless EVs go looking for a different charging service, on average, EVs should wait for about 162.4, 157.9, 147,9, and 142.3 minutes for σ of 60, 120, 180, and 240, respectively. The simulation result shows that 12 MCSs are required for maintaining constant and low waiting time when the number of EVs per charging spot is 18. Both Figs. 10 and 11 show that the smaller the σ value, the higher the waiting time for charging. It is because the interval of EV's request time goes down as the σ value is reduced. If many vehicles are crowded due to a specific event within a short period of time, an additional MCS application may be required for smooth charging service.Applying MCS can enable EVs to charge more efficiently even if they use the same charging point. In addition, the CS can benefit from additional electricity sales through MCS. Fig. 12 shows the electricity sales for each CS when the number of EVs per charging station is 18. The result implies that the CS, which previously had no electricity sales, can sell electricity using MCS. We calculated the Shapley values based on the number of charges and the amount of charge provided by each CS using its MCS, as shown in Table VIII. The number of charges and the amount of charge provided by the MCS correspond to factor 3 and factor 4, respectively.

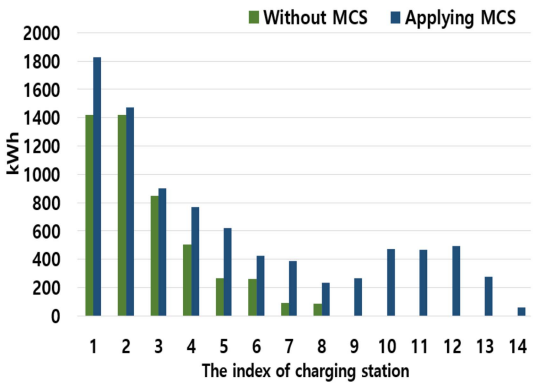

Fig. 12. A change in the charging amount of each CS.

TABLE VIII
THE SHAPLEY VALUE OF EACH CS

The index of CS	The number of charges of MCSs	Total charging amount of MCSs	Shapley Value (Fac3+Fac4)
1	5	413.76	0.0488
2	1	54.70	0.0079
3	1	53.28	0.0078
4	4	264.52	0.0347
5	5	360.34	0.0453
6	3	164.17	0.0237
7	5	301.31	0.0414
8	3	147.11	0.0226
9	4	266.22	0.0348
10	7	472.76	0.0613
11	7	469.00	0.0611
12	8	495.12	0.0671
13	4	276.25	0.0354
14	1	57.22	0.0081

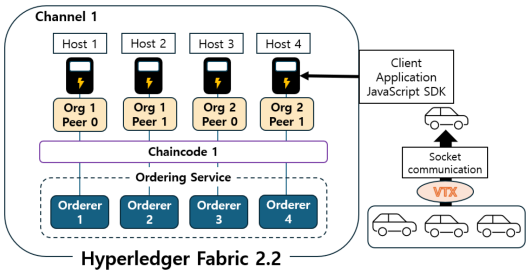

Fig. 13. Overall blockchain architecture.

The Shapley values in Table VIII correspond to 50 % of the total contribution value. CSs with the same charge number have similar Shapley values, as the amount of charge increases proportionally with the charge number. As shown in Table VIII, CSs that actively send the MCS to busy areas have high Shapley values and can have even higher contribution values.

B. Implementation Results

1) Experimental Settings: To evaluate the performance of our blockchain model, we implemented a charging traffic volume blockchain that operates locally by using a private blockchain framework, Hyperledger Fabric 2.2 [49]. Fig. 13 describes the overall blockchain architecture for implementing charging traffic volume blockchain networks, and Fig. 14 shows the experiment setting. We assumed that laptops and

Fig. 14. Experiment setting.

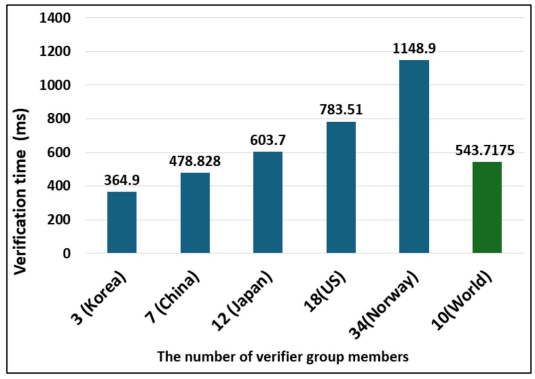

Fig. 15. Transaction reliability verification time.

Personal Computers (PCs) with Intel (R) Core (TM) i7-8700 performance act as charging station servers. There are studies where Raspberry Pi boards have been utilized as Electronic Control Units (ECUs) [54], [55], which is a vehicle controller, and blockchain nodes [56]. Thus, we used a Raspberry Pi 4 Model B with 8 GB RAM as an EV controller for the implementation. In our model, each charging station participated in the Hyperledger Fabric 2.2 [49] as a peer node maintaining the ledger and an ordering node for transaction consensus. Four charging stations communicate using WiFi communications and run the blockchain through Docker containers. EVs participate as verifier group members, reporting charging station information and sharing verification results through socket communication. Transactions are recorded on the blockchain using the JavaScript SDK provided by Hyperledger Fabric 2.2 [49]. We assume that a Go-based Chaincode for recording transactions on the blockchain was deployed beforehand. We executed the blockchain implementation 100 times and calculated the average of the measurements.

2) Experimental Results: First, we measured the verification time of the transaction reported by the vehicle according to the verifier group size. Fig. 15 shows the verification time of the verifier group according to the number of verifier group members. We determined the size of the verifier group by referring to the number of EVs per charging spot in each major country in Global EV Outlook [52]. A reporting vehicle collects agreements from a number rounded up to two-thirds. If the verifier group member is 34, the total verification time is approximately 1,149 ms. In

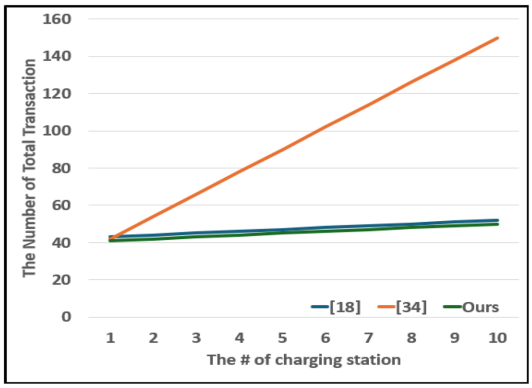

Fig. 16. Transaction overhead comparison for chaincodes.

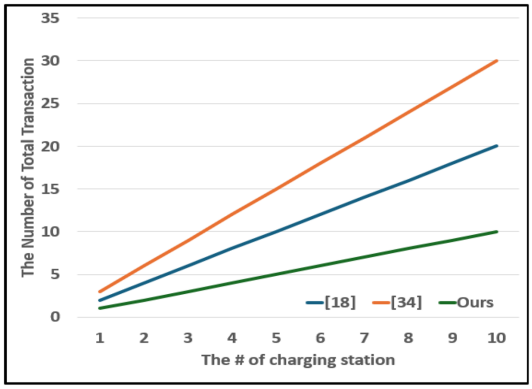

Fig. 17. EV's transaction overhead comparison.

TABLE IX
TRANSACTION LATENCY

The # of transactions per seconds	Recording charging station information (ms)	Querying charging station information (ms)
100	566.3	253.5
200	935.8	429.5
300	1,350.6	588.6
400	1,714.6	795.4

the case of sharing real-time traffic information, this verification time might be considered substantial. However, it is acceptable for charging station information since the typical EV stops during the charging time, and the charging station information update cycle is not frequent. Also, DRIVE AGX Orin [57], which is a vehicle controller released in 2022 for AI processing in autonomous vehicles, is equipped with a CUDA Tensor Core GPU and 12 A78 (Hercules) ARM64 CPUs, along with 32 GB LPDDR5 RAM. Since it has a higher capacity than Raspberry Pi 4 model B with 8 GB LPDDR4 RAM, there will be less communication cost if the EV equipped with DRIVE AGX Orin is a verifier member. The simulation results demonstrated that it has a negligible impact on the efficiency of the proposed model.

Second, we measured the latency when storing and querying transactions in the charging traffic volume blockchain. We assumed that blockchain clients generate 100 transactions per second, and we measured transaction latency by increasing the number of blockchain clients. Table IX shows transaction latency when recording and querying charging station information in the ledger. An increase in the number of transactions leads to

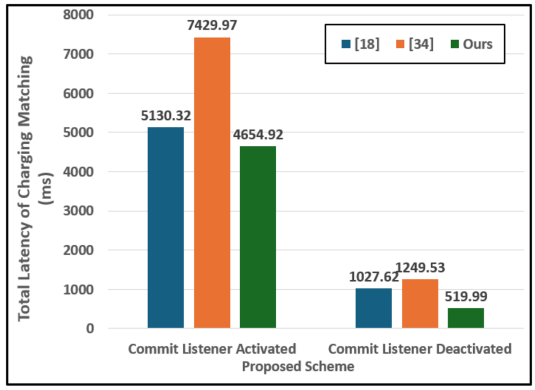

Fig. 18. Comparison of total charging matching latency.

increased transaction latency due to transaction bottlenecks. In the charging scenario, EVs frequently query multiple charging station details rather than recording charging information at large intervals. Therefore, the transaction latency of querying charging information significantly impacts the overall model's efficiency. Reflecting the number of charging spots per EV in Norway [52], even if 34 EVs send 10 transactions per second, the transaction latency remains under one second. Thus, this latency is considered reasonable within actual charging scenarios. When recording charging information, more computing costs are required, resulting in more than twice the latency compared to querying charging information. When the charging information is updated at 400 points per second, it takes less than 2 seconds. The charging station information does not change frequently, so this seems to be an acceptable value.

Finally, we compared the performance of our model with that of previous blockchain-based charging matching protocols between CSs and EVs [18], [34]. Fig. 16 compares the total transaction overhead in the chaincode based on the number of CSs participating in a charging request, with the number of EVs set to 10. As the number of CSs increased from 1 to 10, the number of chaincode transactions in our model and in [18] increased by 22 %, while the number of chaincode transactions in [34] increased by almost 150 %. This seems to be due to the increase in transactions during the bidding phase in [34]. Fig. 17 shows that our model provides the lowest transaction overhead required for EVs as the number of recharges increases among the compared studies. Since EVs have less computing power and memory than CSs or RSUs, it is crucial to reduce the load on EVs when executing chaincode. Consequently, these implementation results show that compared to [18] and [34], the EVs in our proposed model experience lower transaction overhead and reduced computational load during the charging matching process.

Fig. 18 shows the charging matching time of each protocol. We measured performance by separating the cases where the commit listener is enabled or disabled. When the commit listener is disabled, the chaincode transaction completes faster because it does not wait for a save confirmation in the block. According to [34], when the commit listener is enabled, it takes about 7429.97 ms, which is the longest latency. This is likely due to the relatively large number of transactions required during the bidding phase. In comparison, [18] and our proposed method

take 5130.32 ms and 4654.92 ms, respectively, with [18]'s load matching process taking approximately 10.21 % longer. This increased time in [18] seems to be due to the process of reading and updating the reputation score of the CS in the chaincode. The experimental results show that our load matching chaincode is more efficient than previous works [18], [34].

VII. Conclusion

In this paper, we propose a blockchain-based EV charging model considering charging cooperation. The overall charging station information is shared in the charging traffic volume blockchain so that EVs can make optimal charging decisions. To ensure the reliability and credibility of shared information, verifier groups verify the charging station information before deploying. We also suggested a concept of MCS to support a busy CS and provide efficient charging service. We proposed a contribution-based incentive distribution method to motivate EVSPs' participation in the proposed model for effective model operation. The proposed model reduced vehicle charging wait times by 46.9 % in the proposed charging scenario and demonstrated that the transaction verification time is reasonable in actual charging environments. The proposed model addresses the range anxiety issue for long-distance drivers and enables efficient charging services for electric vehicles. As part of future research endeavors, we will investigate optimal charging transaction mechanisms.

References

[1] M. Placek, "Autonomous vehicles worldwide - statistics and facts." Accessed: Apr. 1, 2024. [Online]. Available: https://www.statista.com/topics/3573/autonomous-vehicle-technology/#topicOverview

[2] S. J. Kamble and L. J. Katare, "Self-driving electric vehicle market size, share, competitive landscape and trend analysis report by level of automation, by vehicle type, by type global opportunity analysis and industry forecast," early access: Apr. 1, 2024. [Online]. Available: https://www.alliedmarketresearch.com/self-driving-electric-vehicle-market-A12266

[3] EVBOX, "Connected and in control: A guide to EV charging apps," (n.d). [Online]. Available: https://evbox.com/en/ev-home-charging-station-apps-guide

[4] Y. Chen, Y. Lai, Z. Zhang, H. Li, and Y. Wang, "Malicious attack detection based on traffic-flow information fusion," in *Proc. 2022 IEEE/ IFIP Netw. Conf.*, 2022, pp. 1–9.

[5] M. Waniek, G. Raman, B. AlShebli, J. C..-H. Peng, and T. Rahwan, "Traffic networks are vulnerable to disinformation attacks," *Sci. Rep.*, vol. 11, no. 1, 2021, Art. no. 5329.

[6] L. U. Khan et al., "Federated learning for digital twin-based vehicular networks: Architecture and challenges," *IEEE Wireless Commun.*, vol. 31, no. 2, pp. 156–162, Apr. 2024.

[7] J. Cui, F. Ouyang, Z. Ying, L. Wei, and H. Zhong, "Secure and efficient data sharing among vehicles based on consortium blockchain," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 8857–8867, Jul. 2022.

[8] J. Xiong, R. Bi, M. Zhao, J. Guo, and Q. Yang, "Edge-assisted privacy-preserving raw data sharing framework for connected autonomous vehicles," *IEEE Wireless Commun.*, vol. 27, no. 3, pp. 24–30, Jun. 2020.

[9] Y. Yan et al., "Prediction of traffic flow considering electric vehicle market share and random charging," *J. Adv. Transp.*, vol. 2023, no. 1, 2023, Art. no. 7649689.

[10] Sparkcharge, "Sparkcharge mobile EV charging," early access: Dec. 10, 2022. [Online]. Available: https://www.sparkcharge.io/

[11] ChargeHub, "Chargehub: Tools for electric vehicle drivers in north America." Accessed: Dec. 10, 2022. [Online]. Available: https://chargehub.com/en/

[12] PlugShare, "Plugshare - EV charging station map - find a place to charges." Accessed: Dec. 10, 2022. [Online]. Available: https://www.plugshare.com/

[13] S. Lee and S.-H. Seo, "Design of a two layered blockchain-based reputation system in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 1209–1223, Feb. 2022.

[14] Y. Bai, Q. Hu, S.-H. Seo, K. Kang, and J. J. Lee, "Public participation consortium blockchain for smart city governance," *IEEE Internet Things J.*, vol. 9, no. 3, pp. 2094–2108, Feb. 2022.

[15] Y. Wang et al., "Blockchain-based secure and cooperative private charging pile sharing services for vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 1857–1874, Feb. 2022.

[16] M. Baza et al., "Privacy-preserving blockchain-based energy trading schemes for electric vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 9369–9384, Sep. 2021.

[17] S. Aggarwal, N. Kumar, and P. Gope, "An efficient blockchain-based authentication scheme for energy-trading in V2G networks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 6971–6980, Oct. 2021.

[18] S. M. Danish, K. Zhang, H.-A. Jacobsen, N. Ashraf, and H. K. Qureshi, "BlockEV: Efficient and secure charging station selection for electric vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4194–4211, Jul. 2021.

[19] R. Jin, X. Zhang, Z. Wang, W. Sun, X. Yang, and Z. Shi, "Blockchain-enabled charging right trading among EV charging stations," *Energies*, vol. 12, no. 20, 2019, Art. no. 3922.

[20] L. P. Qian, Y. Wu, X. Xu, B. Ji, Z. Shi, and W. Jia, "Distributed charging-record management for electric vehicle networks via blockchain," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2150–2162, Feb. 2021.

[21] A. Banerjee, M. Clear, and H. Tewari, "Demystifying the role of zk-SNARKs in Zcash," in *Proc. 2020 IEEE Conf. Appl., Inf. Netw. Secur.*, 2020, pp. 12–19.

[22] E. Winter, "The shapley value," *Handbook Game Theory With Econ. Appl.*, vol. 3, pp. 2025–2054, 2002.

[23] L. Liu, H. Zhang, and J. Wu, "A reciprocal charging mechanism for electric vehicular networks in charging-station-absent zones," *IEEE Trans. Mobile Comput.*, vol. 22, no. 2, pp. 621–633, Feb. 2023.

[24] I. D. of Transportation, "Transportation modeling." Accessed: Sep. 28, 2022. [Online]. Available: https://www.in.gov/indot/resources/state-transportation-improvement-program-stip/transportation-modeling/

[25] E. Zavvos, E. H. Gerding, and M. Brede, "A comprehensive game-theoretic model for electric vehicle charging station competition," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 12239–12250, Aug. 2022.

[26] K.-B. Lee, M. A. Ahmed, D.-K. Kang, and Y.-C. Kim, "Deep reinforcement learning based optimal route and charging station selection," *Energies*, vol. 13, no. 23, 2020, Art. no. 6255.

[27] G. Zhou, Z. Zhu, and S. Luo, "Location optimization of electric vehicle charging stations: Based on cost model and genetic algorithm," *Energy*, vol. 247, 2022, Art. no. 123437.

[28] C. B. Saner, A. Trivedi, and D. Srinivasan, "A cooperative hierarchical multi-agent system for EV charging scheduling in presence of multiple charging stations," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2218–2233, May 2022.

[29] F. L. Da Silva, C. E. Nishida, D. M. Roijers, and A. H. R. Costa, "Coordination of electric vehicle charging through multiagent reinforcement learning," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2347–2356, May 2020.

[30] Z. Ding, Y. Lu, K. Lai, M. Yang, and W.-J. Lee, "Optimal coordinated operation scheduling for electric vehicle aggregator and charging stations in an integrated electricity-transportation system," *Int. J. Elect. Power Energy Syst.*, vol. 121, 2020, Art. no. 106040.

[31] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[32] Y. Wang, Z. Su, and N. Zhang, "BSIS: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3620–3631, Jun. 2019.

[33] M. Baza, M. Nabil, M. Ismail, M. Mahmoud, E. Serpedin, and M. A. Rahman, "Blockchain-based charging coordination mechanism for smart grid energy storage units," in *Proc. IEEE Int. Conf. Blockchain*, 2019, pp. 504–509.

[34] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Comput. Sci.- Res. Develop.*, vol. 33, no. 1, pp. 71–79, 2018.

[35] R. Pilling, S. C. Chang, and P. B. Luh, "Shapley value-based payment calculation for energy exchange between micro-and utility grids," *Games*, vol. 8, no. 4, pp. 1–12, 2017.

[36] R. T. Ma, D.-m. Chiu, J. C. Lui, V. Misra, and D. Rubenstein, "On cooperative settlement between content, transit and eyeball internet service providers," in *Proc. 2008 ACM CoNEXT Conf.*, 2008, pp. 1–12.
[37] X. He et al., "A shapley value-based incentive mechanism in collaborative edge computing," in *Proc. 2021 IEEE Glob. Commun. Conf.*, 2021, pp. 1–7.
[38] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, 2002.
[39] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, pp. 36–63, 2001.
[40] G. Wood et al., "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, no. 2014, pp. 1–32, 2014.
[41] D. Huang, X. Ma, and S. Zhang, "Performance analysis of the raft consensus algorithm for private blockchains," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 1, pp. 172–181, Jan. 2020.
[42] A. A. Adewuyi, H. Cheng, Q. Shi, J. Cao, Á. MacDermott, and X. Wang, "CTRUST: A dynamic trust model for collaborative applications in the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5432–5445, Jun. 2019.
[43] S. M. Toolbox et al. *Matlab*. Natick, Massachusetts, USA: Mathworks Inc, 1993.
[44] P. IEA, "Global EV outlook 2022," May 2022. [Online]. Available: https://www.iea.org/reports/global-ev-outlook-2022
[45] L. M. Scott and M. V. Janikas, "Spatial statistics in arcgis," in *Handbook of Applied Spatial Analysis: Software Tools, Methods and Applications*. Berlin, Germany: Springer, 2009, pp. 27–41.
[46] A. Borshchev, S. Brailsford, L. Churilov, and B. Dangerfield, "Multi-method modelling: Anylogic," *Discrete-Event Simul. Syst. Dyn. Manage. Decis. Mak.*, 2014, pp. 248–279.
[47] D. Chen, K. Kang, D. D. Koo, C. Peng, K. Gkritza, and S. Labi, "Agent-based model of electric vehicle charging demand for long-distance driving in the state of indiana," *Transp. Res. Rec.*, vol. 2677, no. 2, pp. 555–563, 2023.
[48] T. Konstantinou et al., "A strategic assessment of needs and opportunities for the wider adoption of electric vehicles in indiana," Purdue Univ. Joint Transp. Res. Program, Tech. Rep. FHWA/IN/JTRP-2022/12, 2022.
[49] S. Shalaby, A. A. Abdellatif, A. Al-Ali, A. Mohamed, A. Erbad, and M. Guizani, "Performance evaluation of hyperledger fabric," in *Proc. 2020 IEEE Int. Conf. Informat., IoT, Enabling Technol.*, 2020, pp. 608–613.
[50] E. V. Database, "Useable battery capacity of full electric vehicles." Accessed: Jan. 2, 2023. [Online]. Available: https://ev-database.org/cheatsheet/useable-battery-capacity-electric-car
[51] E. V. Database, "Energy consumption of full electric vehicles." Accessed: Jan. 2, 2023. [Online]. Available: https://ev-database.org/cheatsheet/energy-consumption-electric-car
[52] P. IEA, "Electric ldv per charging point in selected countries." Accessed: Apr. 4, 2022. [Online]. Available: https://www.iea.org/data-and-statistics/charts/electric-ldv-per-charging-point-in-selected-countries-2010-2021-2
[53] "Electric vehicle time of use rate." Accessed: Nov. 20, 2022. [Online]. Available: https://energycenter.org/thought-leadership/blog/state-electric-vehicle-adoption-us-and-role-incentives-market
[54] Y. Shen, J. Cui, H. Zhong, J. Zhang, I. Bolodurina, and D. He, "A two-layer dynamic ECU group management scheme for in-vehicle can bus," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 8, pp. 10431–10445, Aug. 2024.
[55] T. Lenard, R. Bolboacă, B. Genge, and P. Haller, "Mixcan: Mixed and backward-compatible data authentication scheme for controller area networks," in *Proc. 2020 IFIP Netw. Conf.*, 2020, pp. 395–403.
[56] S. U. Abas, F. Duran, and A. Tekerek, "A Raspberry Pi based blockchain application on IoT security," *Expert Syst. With Appl.*, vol. 229, 2023, Art. no. 120486.
[57] NVIDIA, "Drive agx orin development platform," 2023. Accessed: Nov. 12, 2024. [Online]. Available: https://developer.nvidia.com/drive/agx

Soojin Lee (Student Member, IEEE) received the B.S. degree with the Division of Electrical Engineering from Hanyang University ERICA Campus. Ansan, South Korea, in 2019, and the M.S degree with the Department of Electronic and Electrical Engineering from Hanyang University, Seoul, South Korea, in 2021, where she is currently working toward the doctor's degree with the Department of Electronic and Electrical Engineering. Her research interests include blockchain, IoT security, and privacy protection.

Seung-Hyun Seo (Member, IEEE) received the B.S. degree from the Department of Mathematics, Ewha Womans University, Seoul, South Korea, in 2000, and the M.S. and Ph.D. degrees in computer science from Ewha Womans University, in 2002 and 2006, respectively. She was a Postdoctoral Researcher of computer science with Purdue University, West Lafayette, IN, USA, for two and half years, a Senior Researcher of Korea Internet and Security Agency for two years, and a Researcher for three years in Financial Security Agency, South Korea. She was an Assistant Professor with Korea University Sejong campus, Sejong, China, for two years. She is currently a Professor with Hanyang University, Seoul, South Korea, from 2017. Her research interests include cryptography, IoT security, mobile security, blockchain, and post-quantum cryptography. Her research interests include blockchain, IoT security, and privacy protection.

Kyubyung Kang (Associate Member, IEEE) received the Ph.D. degree in civil engineering from Purdue University, West Lafayette, IN, USA, in 2018, and the M.S. degree from University College London, London, U.K., in 2011. He is currently an Assistant Professor with the School of Construction Management Technology. His research interests include EV charging stations, digital twins, and computer vision applications in construction and infrastructure management.

Qin Hu received the Ph.D. degree in computer science from the George Washington University, Washington, DC, USA., in 2019. She is currently an Assistant Professor with the Department of Computer Science with Georgia State University, Atlanta, GA, USA. She was the Editor/Guest Editor for several journals, the TPC/Publicity Co-chair for several workshops, and the TPC Member for several international conferences. Her research interests include wireless and mobile security, edge computing, blockchain, and federated learning.