Privacy-Preserving Electric Vehicle Charging for Peer-to-Peer Energy Trading Ecosystems

Eman Mohammed Radi, Noureddine Lasla, Spiridon Bakiras
Division of Information and Computing Technology
College of Science and Engineering, Hamad Bin Khalifa University
Email: {eradi, nlasla, sbakiras}@hbku.edu.qa

Mohamed Mahmoud
Dept. of Electrical and Computer Engineering
Tennessee Tech University
Email: mmahmoud@tntech.edu

***Abstract*—The proliferation of renewable energy systems and high-capacity batteries has enabled customers to trade their excess energy on the market in a peer-to-peer manner through the smart grid. At the same time, electric vehicles (EVs) are enjoying widespread acceptance, leading to a higher demand for charging stations. In this paper, we propose a system where energy traders and EV owners collectively work to satisfy the energy demands of EVs. Specifically, energy traders make bids to EV owners who, in turn, reserve their preferred charging station for a specific period of time. To protect the privacy of EV owners, we also introduce an anonymous payment system that cannot link individual owners to specific charging locations. Finally, to guarantee the security and transparency of the entire system, we store all transactions on a consortium blockchain that is managed by the energy traders and the financial institutions that support the anonymous payment system. Our experimental results indicate that the overhead of the cryptographic operations involved in the major transactions is low, in terms of both computational and communication cost.**

I. Introduction

With the global revolution in energy generation, an increasing number of local and distributed renewable energy producers are emerging. This new revolution is driven on the one hand by the global commitment to reduce carbon emission, and on the other hand by the proliferation of customer-sited smart technologies, such as electric vehicles (EVs), solar rooftops, battery storage, etc. The significant potential of EVs in reducing emission levels and fuel consumption has accelerated their wide adoption, and millions of them are expected to join the roads in the next few years [1]. For the continuous operation of EVs without range anxiety, however, a widespread charging infrastructure is needed. To meet this requirement, involving private charging stations, such as home owners powered by locally generated renewable energy, is a natural choice that ensures immediate and low cost charging stations everywhere.

To this end, peer-to-peer (P2P) energy trading [2] is a promising new technology, where customers equipped with high-capacity home batteries trade their excess energy to other customers in a P2P manner through the smart grid. An obvious extension of that approach is to enable energy traders to sell their energy directly to EV owners, by allowing them access to their premises for the purpose of charging. Therefore, in this paper, we introduce a novel energy trading platform for EV charging that (i) protects the privacy of EV owners, (ii) is secure against potential insider or outsider threats, and (iii) eliminates the need for any trusted third parties.

To achieve these goals, we build our system around a blockchain network, where EV owners trade energy directly with local producers without any intermediaries. Blockchain, the technology behind the electronic cash system known as Bitcoin [3], is considered as a key enabler technology for transparent and secure P2P transactional systems. In our system, energy producers publish competitive bids for EV owners to charge their vehicles in their locations, and EV owners accept those bids by reserving the most beneficial offer. For security and transparency, all these operations, along with the subsequent monetary exchange, are performed through the underlying blockchain network. To improve the efficiency and scalability of the system, we choose a *consortium* blockchain where the validators, i.e., nodes with write permission on the blockchain ledger, are known and trusted entities.

Nevertheless, relying on existing payment systems (such as credit or debit cards) for trading transactions may violate the privacy of the EV owners, because their charging locations can be tracked over long periods of time. These locations may reveal potentially sensitive information about the owners, such as habits, workplaces, health issues, etc. On the other hand, utilizing an anonymous payment systems such as Bitcoin and Zcash [4] is not a viable solution, since cryptocurrencies are prohibited or restricted in many countries. Therefore, in this work, we also propose an anonymous payment system that is based on real currency. In particular, it leverages a trusted financial entity to exchange real currency into *digital coins* of the same denomination that are provably untraceable. The underlying protocol is based on the concept of blind signatures that was originally proposed by Chaum [5]. In addition to coin untraceability, our system is secure against unauthorized use of coins, by enforcing a proof of ownership on every spent coin through a zero knowledge proof (ZKP) protocol.

To evaluate the scalability of the proposed P2P energy trading platform, we implemented all the cryptographic operations involved in the major blockchain transactions. The experimental results show that the computational and communication cost is very low, thus having a negligible impact on the underlying blockchain network.

The remainder of the paper is organized as follows. Section II discusses the related work from the literature and

Section III introduces the cryptographic primitives that we employ in our methods. Section IV presents the details of our energy trading platform and Section V discusses its privacy and security characteristics. Section VI presents the results of our experimental evaluation and Section VII concludes our work.

II. Related Work

There has been a plethora of research work in the areas of EV location privacy, anonymous payment systems, and P2P energy trading. However, none of the existing approaches propose a comprehensive solution that can be directly applied to our problem setting. More relevant to our work is the scheme by Knirsch et al. [6], where charging stations issue bids to EV owners in response to their charging requests. To select their preferred charging bids, EVs send hidden commitments to the blockchain that are not verified for double reservations and may, thus, lead to scheduling conflicts. Furthermore, the authors do not propose an anonymous payment method to protect the privacy of the EVs.

Pustisek et al. [7] employ smart contracts to dynamically select the best bids from various charging stations. Nevertheless, their method does not address EV privacy, charging reservations, or the underlying payment mechanism. Pop et al. [8] also utilize smart contracts, but their objective is to manage demand response programs in smart grids. Kang et al. [9] address P2P electricity trading among EVs on the smart grid using a consortium blockchain. Their approach focuses mainly on the underlying auction mechanism and does not address privacy issues. In addition, all EVs have to register their public keys and wallet addresses with the certification authority, which may potentially link payments to specific EVs.

Another line of work regards the privacy-preserving authentication of EVs in vehicle-to-grid (V2G) networks. A common technique is to associate different pseudonyms to the same EV, as in Ref. [10], [11], [12]. On the other hand, Zhu et al. [13] utilize short randomizable group signatures based on bilinear maps, and Zhao et al. [14] leverage a trusted platform module (TPM) along with Camenisch-Lysyanskaya signatures to create anonymous credentials.

An anonymous payment system is essential in any privacy-preserving protocol involving monetary exchange, and numerous methods have incorporated them in their design. For example, Gunukula et al. [15] utilize anonymous coins that are generated with partially blind signatures, which make it impossible to link a charging request to a specific EV owner. Zhu et al. [13] also employ anonymous coupons that are issued by a third-party server, for the payment of parking fees. Similarly, Gao et al. [16] preserve the privacy of EV charging through an anonymous and reliable payment mechanism that leverages the Hyperledger blockchain. An interesting payment scheme is introduced by Au et al. [17] which, in addition to anonymity, it implements a feature called voluntary revocation. That is, given the user's consent, it is possible to trace that user's transactions. Nevertheless, all the aforementioned methods employ a trusted third-party to avoid double spending attacks, which is a single point of failure and a possible target for attackers. In addition, they do not protect against stolen coin attacks.

III. Preliminaries

In this section we present two cryptographic primitives that we utilize in our methods, namely, blind elliptic curve DSA signatures and Schnorr's identification protocol.

A. Blind Elliptic Curve DSA Signatures

The concept of blind signatures was first introduced by David Chaum in 1983 [5] as a means to provide an untraceable payment system. Using a blind signature protocol, the user (*requester*) can get a valid signature for a message M from the *signer*, while keeping M secret. In this work, we leverage the blind signature scheme described in Ref. [18], which is based on an elliptic curve implementation of the digital signature algorithm (DSA). Elliptic curve schemes offer faster computation times with significantly shorter signatures. The aforementioned protocol consists of the following steps.

1) We assume that all parties share the description of an elliptic curve of order n with generator G.[1] In addition, the signer's public key is $P = d \cdot G$, where d is the corresponding private key.
2) The signer selects a uniformly random integer $k \in \mathbb{Z}_n^*$ and sends $R = k \cdot G$ to the requester.
3) The requester selects uniformly random integers $\gamma, \delta \in \mathbb{Z}_n^*$ and computes $A = R + \gamma \cdot G + \delta \cdot P$. Let x be the x-coordinate of point A, and let $t = x \bmod n$. The requester computes $c = H(M||t) \bmod n$ and sends $c' = (c - \delta) \bmod n$ to the signer. $H(\cdot)$ is a cryptographically secure hash function, such as SHA256.
4) The signer computes $s' = (k - c' \cdot d) \bmod n$ and sends the result back to the requester.
5) The requester computes $s = (s' + \gamma) \bmod n$ and stores the signature of M as (s, c).
6) To verify the signature, the *verifier* computes $A = c \cdot P + s \cdot G$. Let x be the x-coordinate of point A, and let $t = x \bmod n$. The verifier checks that $c = H(M||t) \bmod n$.

B. Schnorr's Identification Protocol

An identification protocol allows the owner of a public key (*prover*) to prove to a *verifier*–in zero knowledge–that he indeed knows the value of the underlying secret key. A well-known identification protocol is due to Schnorr [19], which is summarized below for the case of an elliptic curve cryptosystem.

1) We assume that all parties share the description of an elliptic curve of order n with generator G. The prover's public key is $P = d \cdot G$, where d is the corresponding private key.
2) The prover selects a uniformly random integer $k \in \mathbb{Z}_n^*$ and sends $R = k \cdot G$ to the verifier (*commitment*).

[1] Throughout the paper, we use uppercase characters to represent elliptic curve points, and lowercase characters to represent scalars.

3) The verifier selects a uniformly random integer $e \in \mathbb{Z}_n^*$ and sends it to the prover (*challenge*).
4) The prover computes $s = (k + e \cdot d) \bmod n$ and sends it to the verifier (*response*). The verifier accepts, if $s \cdot G = R + e \cdot P$.

Gennaro et al. [20] utilize higher degree polynomials that enable the execution of multiple Schnorr protocol instances at a cost that is very close to the cost of a single instance. The protocol is identical to the one described above, except for the last step. In particular, the prover holds m public keys $P_1, P_2, \ldots, P_m$, corresponding to private keys $d_1, d_2, \ldots, d_m$. When the prover receives the verifier's challenge e, it computes the response s as follows.

$$s = (k + \sum_{i=1}^{m} e^i \cdot d_i) \bmod n$$

The verifier then accepts, if the following is true.

$$s \cdot G = R + \sum_{i=1}^{m} e^i \cdot P_i$$

IV. A P2P Energy Trading Platform for Privacy-Preserving EV Charging

In this section, we describe in detail our energy trading platform that facilitates the privacy-preserving charging of EVs. We first present an overview of the system architecture, followed by the individual protocols for anonymous payments, charging reservation, and EV charging.

A. System Architecture

Fig. 1 shows the system architecture, which consists of the following five entities: certificate authority (CA), trusted financial entity (TFE), charging station (CS), electric vehicle (EV), and consortium blockchain. In the following paragraphs, we discuss the role of each entity in realizing the privacy and security objectives of our system and also describe the underlying threat model.

Certificate authority The role of the CA is to issue public key certificates to (i) the charging stations (either companies or individual home owners) that wish to participate in the EV charging network and (ii) the financial entities involved in the anonymous payment system. This is necessary due to the consortium nature of the underlying blockchain network, which assumes that all parties with write permissions on the blockchain are known and trusted. All public keys are based on an elliptic curve cryptosystem, identical to the one listed in Section III.

Trusted financial entity This is an organization that facilitates the implementation of the anonymous payment system. Specifically, the TFE will (i) sell *untraceable* digital coins to EV drivers to be used as payment to the CS providers and (ii) exchange these coins for real currency on behalf of the CS providers. Note that there could be multiple independent TFEs involved in the system.

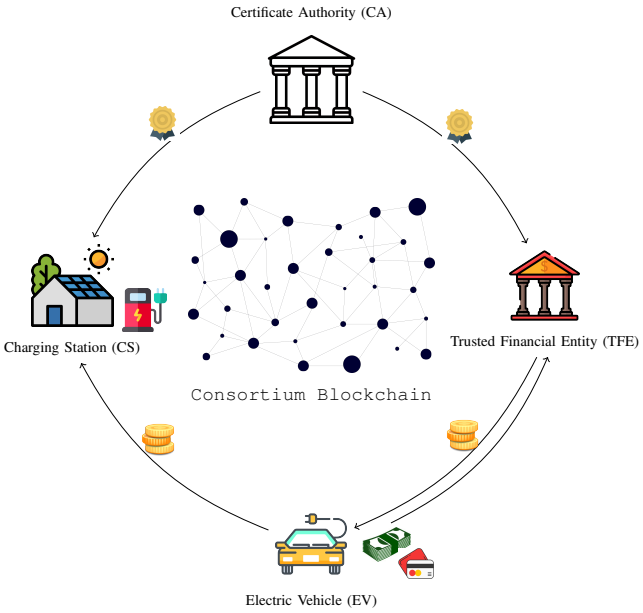

Fig. 1. System architecture

Charging station The CS is an entity that actively participates in the charging operation of EVs. The CS can be a home owner that harvests renewable energy and wishes to trade it on the market or any standard EV charging station that operates today.

Electric vehicle The EV corresponds to the owner of the vehicle that interacts with the system through a web or mobile application. We assume that all operations are performed via the underlying app, so that there is no face-to-face interaction with other entities.

Blockchain At the heart of our architecture is a blockchain network that processes and records all transactions among the different entities. More specifically, the blockchain will handle the following four transactions: *bidding*, *reservation*, *payment*, and *coin to currency exchange*. These transactions are explained in detail in the following sections.

Threat model In this work, we consider three types of attacks, namely attacks against the privacy of the EV owners, the reservation system (denial of service), and the payment system (stolen coins). We assume that all the certified entities (TFEs and CSs) are *honest-but-curious*, i.e., they will execute the protocols correctly, but try to learn more information about the EVs by examining the underlying transcripts. We also allow external *malicious* adversaries that have access to the blockchain and can pose as legitimate EV drivers. These adversaries also have eavesdropping capabilities and can see all the exchanged messages. Finally, we assume that all parties run in polynomial time and are, thus, unable to break the cryptographic protocols.

B. Anonymous Payment System

The anonymous payment system is realized through a trusted entity (TFE) that converts real currency to untracable digital coins and vice versa. Therefore, the first step is for EV drivers to purchase these untracable coins from the TFE, a process that is performed *outside* the blockchain. Specifically, we assume that the application on the EV driver's smart device contains an *e-wallet* service, which stores coins that are digitally signed by the TFE. To guarantee untraceability, all coins have the same *fixed* value, which should be small enough to facilitate any payment (e.g., 5 or 10 cents). Then, the purchasing of digital coins proceeds as follows, where we assume that all parties share the description of an elliptic curve of order n with generator G (as explained in Section III).

1) Suppose the EV driver (client) wants to purchase m digital coins from the TFE. After the payment is made (e.g., through a credit card), the client chooses m secret and uniformly random *serial numbers* $s_1, s_2, \ldots, s_m \in \mathbb{Z}_n^*$ and computes m public keys $M_i = s_i \cdot G, 1 \leq i \leq m$. Each public key uniquely identifies one coin.
2) The client and the TFE invoke the blind signature protocol of Section III, where the client obtains a valid signature $sig_{TFE}(M_i)$ for each purchased coin M_i. The TFE remains oblivious to the values (i.e., public keys) of the individual coins.
3) The digital coins are stored securely in the e-wallet of the client as tuples of the form $\langle s_i, M_i, sig_{TFE}(M_i)\rangle$ and, to ensure privacy, they are not revealed until the client decides to use them as payment.

Note that, to improve the efficiency of our system (by reducing the coin-related operations), we can allow digital coins of larger denominations (e.g., \$1, \$5, \$10). In this case, each coin will be stored as $\langle v, s_i, M_i, sig_{TFE}(M_i, v)\rangle$, where v is the coin's monetary value. However, this approach is prone to privacy leaks if the TFEs monitor the purchasing and spending history of the different denominations.

C. Charging Station Reservation

The reservation process consists of two phases, namely, bidding and selection. The bidding phase is performed by the authorized CS providers, who offer competitive charging prices in order to attract EV drivers to their charging locations. In particular, when a CS provider wishes to place a new bid, it constructs a blockchain transaction (*bidding*) that includes all the necessary information: *bid ID*, *CS public key*, *location*, *timeslot*, *price*, and *max energy* (kWh) that it is willing to provide. The transaction is signed with the private key of the CS and is broadcast on the blockchain network. Before storing the transaction on the ledger, the validators on the blockchain network will verify that the location/timeslot has not been reserved previously. To facilitate the competition among the various providers, we allow bids to be updated in the form of new transactions that invalidate existing ones.

A customer who wants to charge his/her EV, will then query the blockchain to retrieve offers from a certain geographic area. Through their smart devices, customers will select the most appropriate bids, in terms of location, timeslot, and price. To reserve a specific charging location, the customer will create a new blockchain transaction (*reservation*) that includes the selected *bid ID*, the *CS public key*, and a predefined *down payment* (e.g., \$2) in the form of digital coins. Each coin in the transaction is represented with the tuple $\langle M_i, sig_{TFE}(M_i)\rangle$. The transaction is then signed with a *fresh* public key that is generated on-the-fly by the customer, and is finally broadcast on the blockchain network.

The validators will then verify the following: (i) the bid ID is valid, i.e., it has not been updated, (ii) there is no other reservation associated with this bid ID, and (iii) the attached digital coins are valid (the TFE's signatures match) and have not been used previously in other transactions. Once these requirements are verified, the reservation transaction is stored on the ledger. The down payment associated with each reservation is necessary in order to discourage denial of service (DoS) attacks, where an adversary makes fake reservations to block one or more CS providers from getting legitimate customers. Finally, we should point out that the purpose of generating a new (never before used) public key for each reservation is to protect the privacy of the underlying users. In other words, similar to the Bitcoin protocol, EV drivers are not associated with a specific public key and, as such, they do not need to get a public key certificate from the CA.

D. EV Charging

The charging of the EV at the reserved CS is the most complex process in terms of cryptographic operations, because it necessitates numerous invocations of verification protocols. First, when the EV arrives at the charging facility, it has to prove its identity to the CS provider. In particular, the EV and the CS will engage in an instance of Schnorr's identification protocol (Section III), in order for the EV to prove to the CS that it knows the private key corresponding to the public key that made the reservation. Following a successful authentication, the EV will complete its charging within the agreed time frame and and then initiate the payment process.

Payment is achieved by presenting to the CS a series of digital coins of the form $\langle M_i, sig_{TFE}(M_i)\rangle$. Note that, the coins used as down payment in the reservation transaction will become part of the payment. Nevertheless, transmitting the coins to the CS is vulnerable to a *stolen coin* attack, where an adversary that has compromised the CS can terminate the payment protocol and use the coins in other transactions. To thwart such an attack, the EV and the CS will invoke the batch version of Schnorr's protocol [20] so that the EV can prove that it knows the underlying serial numbers of the submitted coins.

To finalize the payment and the entire charging process, the EV will create a new blockchain transaction (*payment*) that includes the following information: *bid ID*, *CS public key*, used *coins* $\langle M_i, sig_{TFE}(M_i)\rangle$, and the *transcript* of the batch identification protocol (commitment, challenge, and response).

The transaction will be signed by both parties (EV and CS) before it is broadcast on the blockchain network. Then, the validators will verify the legitimacy of the payment process, i.e., check that (i) the coins have not been used previously, (ii) the TFE's coin signatures are valid, and (iii) the batch identification protocol is correct. Once the transaction is stored on the blockchain, the ownership of the coins is implicitly transferred to the CS provider. Note that, to guarantee privacy, the coins cannot be reused again to purchase energy by the new ownership, for instance, in case when the CS provider need to charge its own EV elsewhere.

Thus, the last step is for the CS provider to exchange its digital coins for real currency, which is a process that takes place between the CS and the TFE. More specifically, the TFE will transfer the corresponding funds (from a unique payment transaction) to the CS provider's bank account, and the CS will create a new blockchain transaction (*coin to currency exchange*) that includes the blockchain *transaction ID* of the payment and the *amount* of money that was transferred to the CS. This transaction will be signed by both parties and eventually be stored on the ledger.

V. Security and Privacy Analysis

In this section, we discuss possible security and privacy concerns and how our proposal addresses each one of them.

Privacy The privacy of the EV owners (their charging locations, purchased energy, etc.) is protected by (i) the use of random *pseudonyms* for charging reservations that correspond to fresh public-private key pairs, and (ii) the anonymous payment system. Every random pseudonym expires once the driver completes the charging process, which ensures transaction *unlinkability*. Moreover, the coins used as payment are untraceable and are only linked to the EV's current pseudonym. Finally, each coin can be used exactly once, which is guaranteed by the blockchain validators.

Security As the system is open to public access (for EV owners), it is exposed to attacks causing denial of service for legitimate users. To discourage such attacks, each reservation transaction is required to submit a predefined down payment, which is large enough to make DoS attacks expensive. Any transaction that does not include the down payment is automatically rejected by the blockchain validators. We also protect against stolen coins by a compromised CS, through a verification step at the payment process. Specifically, the spender of a digital coin has to prove with a ZKP protocol that it knows the coin's serial number (without revealing it). Any coin that is not verified is rejected by the blockchain network.

Finally, our system ensures a transparent trading platform by offering a fair access to the bidding process. Thanks to blockchain technology, no single entity or authority can monopolize the system for its own benefit. The rules for transaction validation are predefined and executed in a completely distributed manner through a consensus protocol, and no single point of failure can be exploited by an external or internal entity. For instance, a double reservation attack or a double coin spending attack can be easily detected and rejected by the network.

VI. Performance Evaluation

We implemented all cryptographic protocols involved in our methods with the C programming language, using OpenSSL's library for elliptic curve cryptography, and run our code on a 2.8 GHz Intel Core i7 CPU. For 128-bit security, we selected ANSI's *X9.62 Prime 256v1* curve, whose order n is a 256-bit prime. In the next sections we describe the overhead of these protocols in terms of computation and communication.

A. Computational Cost

Table I shows the CPU time that is required for the cryptographic protocols at the different entities. Clearly, the operations involved are very efficient, and, more importantly, the signature verification that is executed on the blockchain necessitates just 0.017 msec/coin. As a result, even transactions with thousands of exchanged coins can be verified within milliseconds.

TABLE I
Computational Cost

Protocol	CPU time (msec)
Coin purchase – one coin (EV)	0.323
Coin purchase – one coin (TFE)	0.094
Signature verification (CS/blockchain)	0.017
Schnorr identification – prover (EV)	0.084
Schnorr identification – verifier (CS)	0.255

Fig. 2 illustrates the efficiency of Schnorr's batch protocol in verifying the ownership of a large number of coins. For example, verifying 1000 coins individually requires 140 msec at the prover and 280 msec at the verifier, whereas the batch protocol reduces these costs to 0.1 msec and 68 msec, respectively.

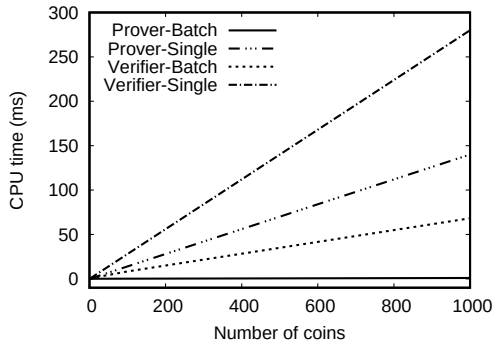

Fig. 2. Effect of Schnorr's batch protocol on CPU time

B. Communication Cost

The communication cost of the cryptographic protocols is very low, due to the underlying elliptic curve cryptosystem. In particular, the transmission of an elliptic curve point incurs

64 bytes of communication, while scalar values require the transmission of just 32 bytes. As depicted in Table II, both coin purchase and Schorr's identification protocol are executed with 128 bytes of communication (one elliptic curve point and two scalars).

TABLE II
COMMUNICATION COST

Protocol	Communication cost (bytes)
Coin purchase – one coin	$64 + 32 + 32 = 128$
Schnorr identification	$64 + 32 + 32 = 128$

Finally, Fig. 3 shows the effect of Schorr's batch protocol on the communication cost. As described in Section III, the batch protocol involves the exchange of the same type of messages as the original protocol, so the communication cost is constant with respect to the number of coins (128 bytes). On the other hand, the cost of executing individual instances of Schnorr's protocol incurs a cost that grows linearly with the number of coins.

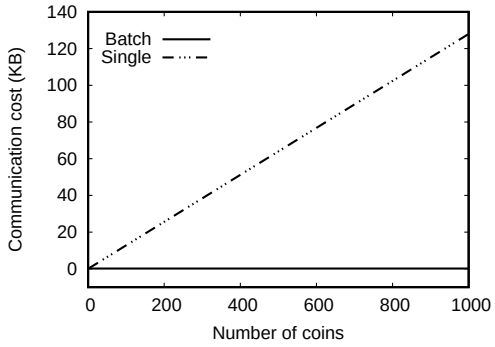

Fig. 3. Effect of Schnorr's batch protocol on communication cost

VII. CONCLUSIONS

In this paper, we proposed a P2P energy trading platform that enables customers to trade their excess energy directly with EV owners, by offering charging services on their premises. The system is built on top of a consortium blockchain that provides security and transparency without the need of a trusted third party. To preserve the privacy of EV owners, we also introduced an anonymous payment system that allows EVs to pay their charging fees with untraceable digital coins. Furthermore, we have incorporated several security features in our design that defend against denial of service and stolen coin attacks. Our preliminary implementation of the underlying cryptographic primitives illustrates that the effect of the cryptographic protocols on the trading platform is negligible. In our future work, we will implement a proof-of-concept system of the entire trading platform that interacts with users through a mobile application. We will also extend our work to consider *dynamic* EV charging, where EVs are charged while driving on road segments equipped with specialized charging pads.

REFERENCES

[1] C. Fiori, K. Ahn, and H. A. Rakha, "Power-based electric vehicle energy consumption model: Model development and validation," *Applied Energy*, vol. 168, pp. 257–268, 2016.

[2] W. Tushar, C. Yuen, H. M. Rad, T. K. Saha, H. V. Poor, and K. L. Wood, "Transforming energy networks via peer-to-peer energy trading: The potential of game-theoretic approaches," *IEEE Signal Processing Magazine*, vol. 35, no. 4, pp. 90–111, 2018.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[4] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *2014 IEEE Symposium on Security and Privacy*, May 2014, pp. 459–474.

[5] D. Chaum, "Blind signatures for untraceable payments," in *Proc. Advances in cryptology (CRYPTO)*, 1983, pp. 199–203.

[6] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Computer Science - R&D*, vol. 33, no. 1-2, pp. 71–79, 2018.

[7] M. Pustisek, A. Kos, and U. Sedlar, "Blockchain based autonomous selection of electric vehicle charging station," in *Proc. International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)*, 2016, pp. 217–222.

[8] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 1, p. 162, 2018.

[9] 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 Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154–3164, 2017.

[10] S. Afrin and A. Kwasinski, "A privacy-preserving method with flexible charging schedules for electric vehicles in the smart grid," in *Proc. IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2017, pp. 1–6.

[11] V. T. Kilari, S. Misra, and G. Xue, "Revocable anonymity based authentication for vehicle to grid (V2G) communications," in *Proc. IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2016, pp. 351–356.

[12] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "Roaming electric vehicle charging and billing: An anonymous multi-user protocol," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2014, pp. 939–945.

[13] L. Zhu, M. Li, Z. Zhang, and Z. Qin, "ASAP: An anonymous smart-parking and payment scheme in vehicular networks," *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2018.

[14] T. Zhao, C. Chen, L. Wei, and M. Yu, "An anonymous payment system to protect the privacy of electric vehicles," in *Proc. International Conference on Wireless Communications and Signal Processing (WCSP)*, 2014, pp. 1–6.

[15] S. Gunukula, A. B. T. Sherif, M. Pazos-Revilla, B. Ausby, M. Mahmoud, and X. S. Shen, "Efficient scheme for secure and privacy-preserving electric vehicle dynamic charging system," in *Proc. IEEE International Conference on Communications (ICC)*, 2017, pp. 1–6.

[16] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," *IEEE Network*, 2018.

[17] M. H. Au, J. K. Liu, J. Fang, Z. L. Jiang, W. Susilo, and J. Zhou, "A new payment system for enhancing location privacy of electric vehicles," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 1, pp. 3–18, 2014.

[18] Q. ShenTu and J. Yu, "A blind-mixing scheme for bitcoin based on an elliptic curve cryptography blind digital signature algorithm," *CoRR*, vol. abs/1510.05833, 2015. [Online]. Available: http://arxiv.org/abs/1510.05833

[19] C. Schnorr, "Efficient signature generation by smart cards," *J. Cryptology*, vol. 4, no. 3, pp. 161–174, 1991.

[20] R. Gennaro, D. Leigh, R. Sundaram, and W. S. Yerazunis, "Batching schnorr identification scheme with applications to privacy-preserving authorization and low-bandwidth communication devices," in *Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*, 2004, pp. 276–292.