2020 IEEE 17th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET) | 978-0-7381-0527-7/20/$31.00 ©2020 IEEE | DOI: 10.1109/HONET50430.2020.9322826

Efficient and Secure Energy Trading in Internet of Electric Vehicles Using IOTA Blockchain

Mudassir Ali
Department of Computer Science
COMSATS University Islamabad
Islamabad 44000, Pakistan
Email: mudassir.ktk6@gmail.com

Adeel Anjum
Department of Computer Science
COMSATS University Islamabad
Islamabad 44000, Pakistan
Email: adeelanjum2001@hotmail.com

Adnan Anjum
IBM
Pakistan
Email: adnananjum@live.com

Muazzam A. Khan
Department of Computer Science
Quaid-i-Azam University
Islamabad 44000, Pakistan
Email: khattakmuazzam@gmail.com

***Abstract*—The Internet of Electric Vehicle (IoEV) energy trading is where the Electric Vehicles (EVs) provide energy to vehicles, grids, community, and buildings. A scalable, efficient, secure, and best price selection scheme is needed that supports the IoEV energy trading transaction. The traditional blockchain is used in the existing researches to achieve these needs. This paper proposes an efficient and secure energy trading scheme in IoEV energy trading using the IOTA blockchain. EVs privacy protection algorithm is proposed in which somebody cannot track EV's exact position. The Stackelberg game theory technique is used to select the best seller at a given time slot and to perform the negotiation between buyers and sellers on the energy price in an off-blockchain manner. The empirical analysis shows that the proposed scheme performs better than the traditional techniques in terms of efficiency, privacy, and energy price.**

I. Introduction

The uncontrolled EVs charging gives significant challenges to the quality of power that incurs major losses and high loads. Smart management of energy enables to develop a city that is maintainable, green and smart [1], [2]. However, smart management of energy faces challenges because of the non-participation of EVs in energy trading and the intermittent nature of renewable sources of energy. Specifically, the increase of demand response (DR) is explored in order to balance the load that enables consumers to adjust their energy consumption with the cost [3]. In peak hours, the cost of energy is high because of high consumption and low production. IoEV based energy trading plays a major role to reduce the demand-response load in peak hours without using additional storage and production resources [4]. IoEV is a general form of vehicle to vehicle (V2V), vehicle to grid (V2G), vehicle to the community (V2C), and vehicle to building (V2B). The electric vehicles have the surplus energy, but they are reluctant to participate in the process of energy trading due to insecure energy transactions. Most of the centralized system is introduced to assure the security of the transaction, and control scheduling of EV. The centralized system faces the problem of failure of a single point, the threat of privacy and anonymity due to hidden danger in a centralized system, and the centralized system is not efficient to control the schedule the larger number EVs, i.e., many EVs needs energy urgently to complete their travel. The best solution to store the transaction in distributed manner is the use of blockchain based techniques. Blockchain plays an important role that provides a secure platform of peer-to-peer energy trading and maintains the energy trading transaction in a distributed manner. Many researchers use the blockchain technology to perform energy trading securely [5], [6]. Blockchain provides storage and data processing in a decentralized and distributed manner without relying on third parties. Since blockchain is immutable, the transactions cannot be changed. Blockchain stores records permanently. Hence, the characteristic of blockchain is shown to be highly beneficial in the distributed IoEV. The generic blockchain faces some drawbacks such as algorithms of consensus, probabilistic nature, growth limitation, and latency of transaction confirmation [7], [8]. Also, the generic blockchain is not suitable for micro-transaction due to the incentives given to the miners end up with higher cost than the value of the transaction. Different researchers use different consensus algorithms to control the shortcoming of generic blockchain such as proof of reputation (POR), proof of stack (POS). However, these algorithms are based on the proof of work (POW) consensus algorithm. We cannot make the new system by using proof of stack consensus (POS) only since POS is shown to be insecure in such cases. We must first use POW to determine which miner has a higher stake and then we can use the POS technique. POW is a computationally intensive consensus algorithm thereby increasing the computational cost [9]. In this paper, we use the IOTA blockchain. Directed acyclic graph-based (DAG) techniques are used in the IOTA blockchain to perform the P2P energy trading [9]. There is no need of miners in IOTA blockchain [10]. IOTA blockchain has less latency and needs less power as compared to the traditional blockchain. IOTA blockchain also provides the same security and distributed ledger as traditional blockchain but it does not incur any

978-0-7381-0527-7/20/$31.00 ©2020 IEEE

transaction fee and supports micro-transactions [11]. So IoTA blockchain is best suited for IoEV energy trading. To sum up, our main contributions are as follows:

1) IOTA blockchain-based IoEV electricity trading scheme is proposed where buyers and sellers negotiate in the network on electricity price.
2) EVs privacy protection model is proposed in which somebody cannot track EVs exact position.
3) Off-blockchain is used in the proposed scheme to perform the negotiation between buyers and sellers.
4) The techniques of Stackelberg game theory is used in the proposed scheme to select the best seller among the various sellers.
5) The simulation of the proposed scheme is implemented, and the analysis of the proposed scheme shows that it performs better than the traditional scheme.

II. Related Work

This section summarizes the latest work related to IoEV energy trading schemes.

The authors in [12]–[16] use the blockchain based techniques to build a secure system and protect the privacy of buyers and seller and to participate in the process of trading. In [12], the authors proposed a blockchain-based framework for general and realistic P2P trading of data. The consortium blockchain is used with iterative double auction mechanism, which encourages the participants to participate in the data trading process thereby protecting the seller's and buyers' privacy. The results show the efficiency of the proposed algorithm and also match the market approach as well. However, the proposed algorithm does not consider the micro transactions. In [13], the authors proposed an energy blockchain that performs energy trading securely. They used a scheme of payment that is based on credit which supports trading of enegy frequently and enables fast payment and diminishes the delays of transaction confirmation. The authors in [13] also use the Stackelberg game in credit-based loans for the strategy of optimal price and to maximize the utility of credit bank. The result of the proposed system shows that the scheme of payment that is based on credit and energy blockchain is efficient and effective for the trading of energy. However, the proposed scheme did not consider the strategy for the optimal selection of energy aggregators. In [14], the authors proposed a localized P2P electricity trading system with consortium blockchain (PETCON). The authors use consortium blockchain with an Iterative double auction mechanism to achieve secure and trustful electricity trading and optimize electricity pricing and maximize social welfare. The results show that the proposed method improves the privacy and security of the transaction. However, the proposed scheme did not consider the micro transaction for electricity trading. In [15], a noise-based privacy-preserving approach is proposed to hide the trading distribution trends for the blockchain-enabled neighboring energy trading system. The authors use the noise core algorithm with a privacy-preserving mechanism. The proposed approach defends all the adversaries and device-identity linking attacks, which are assumed in the threat model. However, this work is only used for energy trading in smart grids. We can also extend this work for IoV, IoEV. In [16], the authors proposed the anonymous and fair blockchain-based scheme for the dissemination of ad, which protects the privacy of vehicle and facilitates fair incentives. The authors use smart contract and Markle hash tree for the proof of ad receiving (POAR). It tackles different attacks such as the attacks of "double-claim" and "free-riding". However, the proposed scheme efficiency can be improved by using batch verification that perform the proofs of aggregation dissemination.

III. Proposed System

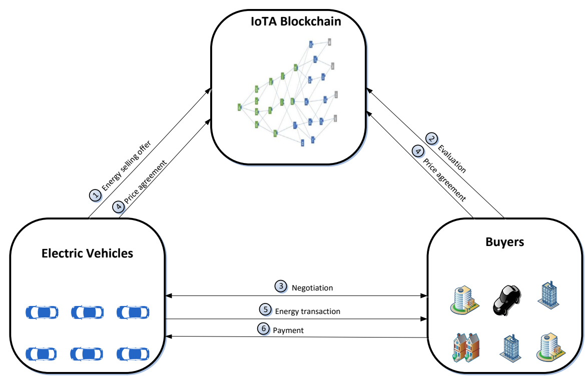

Fig. 1: The IoEV energy trading process using IOTA blockchain.

Fig. 1 shows the process of the proposed technique. First, the selling energy EVs send their selling energy with a price to the IOTA blockchain. Buyers evaluate the different selling energy offers of selling energy EVs to select the best possible selling energy EV in the given time. When the buyer selects the best selling energy EV for them, buyers do the negotiation with it on the price of energy in an off-blockchain manner. After negotiation, when both buyer and seller agree on the price, then buyers send the price agreement to the IOTA blockchain and selling energy EV verify that price agreement. After confirmation of a price agreement, then the selling energy EV starts the transaction of energy on the basis of the agreed price. In the proposed system, smart contract work as an aggregator that supports the communication between the buyers and sellers.

A. Privacy-preserving model for EV

The main aims of this protocol are presented as follows.

1) EV exact position cannot be fined by any participants in the IoEV energy trading.
2) The buyer and seller decision information on the energy price should not be known to any participants.
3) The exact location of EVs somebody cannot be tracked in real-time.

The ID is used in the blockchain for the participants' identification, so the blockchain participants are anonymous. Transactions and keys relating to participants give the possibility of deanonymizing [17]. Thus for every EVs selling offers of energy, id changed and created a new pair of key that reduce deanonymizing. EV privacy-preserving protocol uses IOTA blockchain technology. This protocol consists of four phases. The EV identification in the IOTA blockchain is represented by ID ζ. The buyer is represented by i. The parameters that the vehicle used for the energy offer are e, t, r, p. Here, we used e for energy, t for the time slot, r for the region, p for price. The four phases we used in the proposed protocol to find the best possible seller of energy. The four phases are the Bidding phase, Evaluation phase, Negotiation phase, and charging phase.

1) Bidding phase: The EVs offer of energy selling is placed in this phase with identity to the buyers. The offers of energy selling contain the amount of energy $e \in Q_+$, time slot $t \in T$, range $r \in R$, and price p. The EV should choose the region broadly within possible range so that EV privacy is protected. The participants will not be able to find beyond the ID ζ and offers of selling energy (e, t, r, p). The ID changed with every offer of selling energy, so it is not easy to track the EVs with multiple energy selling offers. The value of (e, t, r, p) contains a different value with multiple offers of energy selling, so the participant will not be able to find the exact location of EV by using these parameters. The offer of energy selling is also not related directly to the specific EV because of the only offers of energy selling, and the ID shows to the participants. The current position of EV does not include in it, and only the region of EV show to the buyers. The EVs offers of energy selling are showed to all the buyers when the offers are submitted to the IOTA blockchain.

2) Evaluation phase: The buyers evaluate the EVs different offers of energy selling in this phase based on their supply of energy, price, and distance. For instance, the buyers may not prefer the EVs with the lowest price because of the energy supply and distance and choose the higher price EVs because of the nearby distance. When more buyers demand come to EV, then it depends on the EV that which one is best suitable for it to take the decision. EVs may prefer buyers who have parking facilities and nearby shops and EVs owners during the process of discharging done the shopping.

Buyers decide privately in an off-blockchain manner. This decision information is not shown to any participant in IoEV energy trading. So nobody knows the price of energy bought and sold. Thus value is published to the IOTA blockchain in the form of hash by hiding and binding commitment. So the EV decision rebuilding is impossible if the decision shows publicly in the IOTA blockchain.

3) Negotiation phase: The buyers communicate with energy selling EV in off-blockchain manners about the energy price. When both agree on the energy price, then the agreed price is published in the IOTA blockchain, and the energy selling EVs sign on the agreed price. EVs selling offers of energy contain the (e, t, r, p), and the buyer evaluates these values to select the best possible EVs of energy selling for energy buying. When suitable EV of energy selling found, then buyer creates their bids function $bi = f(e, t, p)$. This bidding function represents that buyer i is the desire to buy energy e from EV at time slot t for $bi \leq bj, j = 1, ..., N$. If the seller agrees on the given buyer bid bi, then it is written to the IOTA blockchain.

The blockchain feature of immutability makes the agreeing bid more transparent and reliable. The immutability of agreeing bids prevents the buyer and seller from denying services. For instance, the buyer or seller may say that I did not commit this price.

The negotiation process continued until the seller, and buyer's price converges or passed a certain amount of time. The bidding process depends on the seller or buyer price; if sellers and buyers agree on the first bidding, it takes lower time, or may the seller or buyer offer to update the price at the possible level. If the buyer accepts the seller price on the first bid, it motivates the seller that the price is a suitable price at the given time.

When the buyer and selling energy EV agreed on energy suitable price, buyers computationally binding the commitment $c = H(\zeta, \bar{i}, p, r)$ and generate a transaction, and the selling energy EV digitally sign on it. The commitment binding contains the buyer ID i, seller ID ζ, and the commitment price p and puts the freshly random number with it. This decision information does not show the decision information to participants because of the one-side hash property. This information also does not allow the participant to know the specific EV through this decision.

4) Charging phase: In this phase, the buyer and seller commitment are open by sending the $\zeta, \bar{i}, r$, and p to confirm the selected buyer. The seller and the buyer communicate directly without involving the IOTA blockchain. The buyer confirms $H(\zeta, \bar{i}, r, p) = c$ and checks the time frame that whether it matches the offer time frame of the seller. The energy e transfers to the buyer at the time frame on the price of commitment bi, if commitment and time-frame are valid. This process of energy transaction is only accomplished between the chosen selling energy EV and buyer. The true position is revealed to the buyers at this stage. EV reveal the ID ζ at this stage, and other participants cannot use the same identity because of the property of the cryptographic hash function. When the phase of charging is completed, then the ID of the EV changed.

IV. Game Theory in IoEV Energy Trading

The proposed system consists of multiple seller EVs and multiple buyers (homes, buildings, and EVs). Let $M = \{1, 2, 3, ..., m, ..., M\}$ denotes the total number of sellers where $m \in M$ and $N = \{1, 2, 3, ..., n, ..., N\}$ denotes the total number of buyers $n \in N$. Let $T = \{1, 2, 3, ..., t, ..., T\}$ denotes the time slot where $t \in T$ and it is divided equally, i.e., $\Delta t = 1$. Selling energy EVs place their energy supply and its prices at time t in the IOTA blockchain, then each buyer competes to select the best possible selling energy EVs.

The supply to demand ratio is determined by using the following equation [11].

$$m_r = \frac{S_m^t}{D_n^t} \quad (1)$$

Here, S_m^t represents the seller m supply at time t, and D_n^t represents the buyer n demand at time t. If the value of m_r is equal to or greater than 1, then the actual value to select the best selling energy EV at the given time t as follows.

$$B_{true} = (S_{m,sell}^t)p_m^t + \Lambda_n^t \quad (2)$$

Where the price of the distance is calculated from the following equation

$$\Lambda_n^t = (C_k)(d_{m,k}^t)(p_m^t). \quad (3)$$

Here, Λ_n^t represents the total distance price, C_k represents the consumption of energy per kilometre, $d_{m,k}^t$ represents the distance of selling EV at time t. p_m^t represents seller enforced price at time t.
If the value of m_r is lower than 1, then the buyer's true value to select the best selling energy EV at time t is given as follows.

$$B_{true,l} = (S_{m,l}^t)(p_m^t) + B_{true} \quad (4)$$

Where

$$S_{m,l}^t = S_m^t - D_n^t \quad (5)$$

where $S_{m,l}^t$ represents how much supply of selling energy EV is less than demand D_n^t. Here we found the two groups. Group first, in which supply is greater or equal to demand, and the group second, in which supply is less than demand. It depends upon the buyers, which one it prefers supply or price. If the buyer prefers the price, then the buyer finds the best-selling energy EVs with minimum price and nearby distance in these two groups. After finding the last best-selling energy EVs in these two groups, then the buyer compares these two EVs of different groups. EV_1 is the EV whose supply is higher or equal to the demand, and EV_2 is the EV whose supply is lesser than demand. The buyers compare the EV_1 and EV_2 total price.

$$EV_1 \leq EV_2 \quad (6)$$

It should be noted that both group EVs prices are calculated from the equation 2 and equation 4. In case if both groups of EVs contain the same price, then the buyer selects the group first EV, which is EV1. Another case is that if more than one EVs comes with the same price in the same group, then the buyer goes for negotiation to select the best selling energy EV among the selling energy EVs. In case buyers prefer supply, then buyers ignore the group second, whose supply is lesser than the demand, and only choose the best selling energy from the group first, whose supply is greater than the demand.

V. Performance Evaluation

We conduct performance evaluations to validate the efficiency and effectiveness of the proposed system. We used python v3.6 and solidity for the system performance checkout. In the proposed system IoEV energy trading, we considered the $k-1$ buyers and k sellers to evaluate the system performance. The seller is EVs, which has installed a solar system and EVs trade the surplus energy with buyers (homes, buildings, community, and EVs) to get IOTA coin.

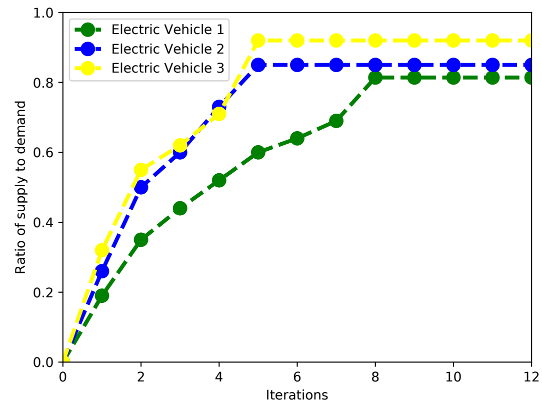

Fig. 2: Supply to demand ratio of EVs.

Fig. 2 shows the supply to demand ratio of three EVs with a number of iterations [11]. EVs increase the selection probability by increasing its supply to adjust the supply to demand ratio. Here we show the three EVs that increase their supply with the number of iteration to adjust the demand ratio. The increment in the supply increases the selection and also the revenue of the EVs.

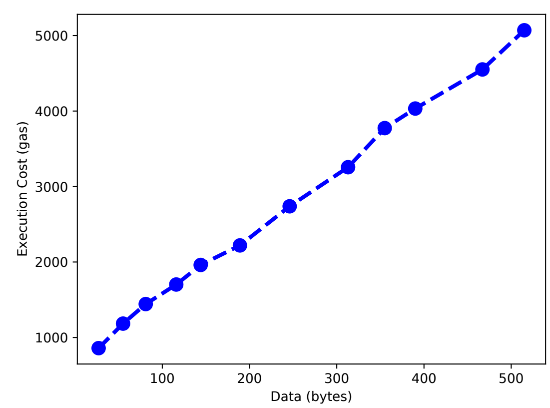

Fig. 3: Data size and its cost of execution.

Fig. 3 shows the data size and the cost of execution. It is observed from the graph that when the data size is increasing, then the cost of execution is increasing. It damages the system performance when all the process of auction of IoEV energy trading is done on the blockchain.

Fig. 4 show the price comparison of five EVs between the traditional first bid scheme and proposed scheme. The graph shows that the five EVs prices are reduced in the proposed

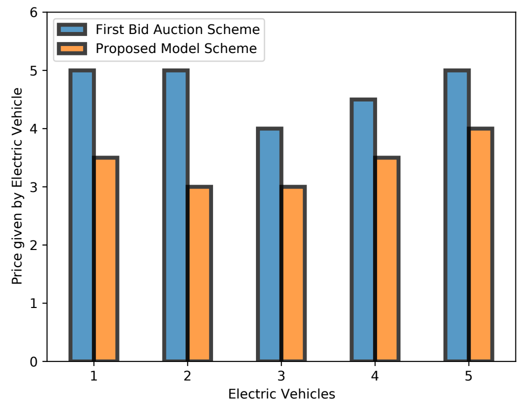

Fig. 4: First Bid Auction Scheme and Proposed Scheme price comparison.

scheme, which increases the SW of the proposed IoEV energy trading scheme.

VI. Conclusion

We propose the efficient and secure energy trading scheme in IoEV energy trading using IOTA blockchain. Game theory is used to select the best possible EVs at time t slot. The off-blockchain is proposed in the proposed scheme to perform the negotiation between buyers and sellers on the price of energy. EVs privacy protection algorithm is proposed in which somebody cannot track EVs exact position. The techniques of Stackelberg game theory is used in the proposed scheme to select the best selling energy EV among the different selling energy EVs at the given time. The proposed scheme simulation result is presented, and the analysis proves that the proposed scheme performs better than the traditional technique in term efficieny, privacy, and price. We can extend this work further to the network of the grid to grid, and grid to vehicle.

References

[1] N. Kumar, A. V. Vasilakos, and J. J. Rodrigues, "A multi-tenant cloud-based dc nano grid for self-sustained smart buildings in smart cities," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 14–21, 2017.

[2] Z. Zhou, J. Feng, B. Gu, B. Ai, S. Mumtaz, J. Rodriguez, and M. Guizani, "When mobile crowd sensing meets uav: Energy-efficient task assignment and route planning," *IEEE Transactions on Communications*, vol. 66, no. 11, pp. 5526–5538, 2018.

[3] Z. Zhou, C. Sun, R. Shi, Z. Chang, S. Zhou, and Y. Li, "Robust energy scheduling in vehicle-to-grid networks," *IEEE Network*, vol. 31, no. 2, pp. 30–37, 2017.

[4] A.-H. Mohsenian-Rad, V. W. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia, "Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid," *IEEE transactions on Smart Grid*, vol. 1, no. 3, pp. 320–331, 2010.

[5] Y. Zhang, C. Xu, N. Cheng, H. Li, H. Yang, and X. Shen, "Chronos+: An accurate blockchain-based time-stamping scheme for cloud storage," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 216–229, 2019.

[6] Y. Zhang, C. Xu, J. Ni, H. Li, and X. S. Shen, "Blockchain-assisted public-key encryption with keyword search against keyword guessing attacks for cloud storage," *IEEE Transactions on Cloud Computing*, 2019.

[7] M. Walport *et al.*, "Distributed ledger technology: Beyond blockchain," *UK Government Office for Science*, vol. 1, pp. 1–88, 2016.

[8] W. Jiang, H. Li, G. Xu, M. Wen, G. Dong, and X. Lin, "Ptas: Privacy-preserving thin-client authentication scheme in blockchain-based pki," *Future Generation Computer Systems*, vol. 96, pp. 185–195, 2019.

[9] S. Popov, "The tangle," *cit. on*, p. 131, 2016.

[10] V. Hassija, V. Saxena, and V. Chamola, "Scheduling drone charging for multi-drone network based on consensus time-stamp and game theory," *Computer Communications*, vol. 149, pp. 51–61, 2020.

[11] V. Hassija, V. Chamola, S. Garg, N. G. K. Dara, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in v2g network," *IEEE Transactions on Vehicular Technology*, 2020.

[12] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A secure and efficient blockchain-based data trading approach for internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9110–9121, 2019.

[13] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE transactions on industrial informatics*, vol. 14, no. 8, pp. 3690–3700, 2017.

[14] 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.

[15] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3548–3558, 2019.

[16] M. Li, J. Weng, A. Yang, J.-N. Liu, and X. Lin, "Toward blockchain-based fair and anonymous ad dissemination in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11 248–11 259, 2019.

[17] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in *Security and privacy in social networks*, Springer, 2013, pp. 197–223.