Blockchain-Based Energy-Trading Systems

Subjects: Energy & Fuels
Contributor: Prince Waqas Khan

Blockchain is the underlying technology of cryptocurrencies, but they provide many other application areas, such as reliable machine-to-machine automatic transactions, including auctions, bidding, and payments. Nowadays, many researchers use blockchain in different electric vehicles' transportation systems, such as payment systems, charging systems, and energy trading systems.

Keywords: electric vehicles ; energy trading ; blockchain

1. Background

As the distribution rate of electric vehicles is shortly expected to become high, Perez et al. [1] addressed the participation of large electric vehicles in the electricity market. They proposed a solution for a situation where several days before purchasing energy, several independent and selfish electrical units entered the market to meet customers' driving needs. In such a case, an independent offer may unnecessarily increase prices, thereby raising the price of electricity for all participants. Cooperation between consolidators will help alleviate this situation by creating coordinated bids. Despite this, this is difficult due to the aggregator's selfish character, and the collector may attempt to manipulate the system for personal gain. To address this, they have used mechanism development technology to develop a coordination mechanism that encourages selfish power generators to truly reflect their energy needs to third-party coordinators. The coordinator can then use the daily bidding algorithm to optimize global bidding to extend smart bidding benefits to a set of competing EV aggregators. The suggested coordination mechanism must be easy to execute and does not necessitate supplementary infrastructures.

The article by Hu et al. aims to solve security problems for Internet of Vehicles (IoV) communications and create consensus and authentication nodes for Intelligent transportation system (ITS) vehicles. With the lack of central nodes and the increasing complexity of IoV's services, Blockchain and IoV can be integrated to create a decentralized communication and consensus mechanism. Blockchain-based IoV architecture complements information communication and consensus authentication using Byzantine consensus algorithms based on timeline and rumor protocols. The empirical results prove that the algorithm is superior to traditional authentication techniques in terms of IoV information security and consensus performance. Furthermore, the findings provide a comparative solution to the problem of IoV certification for intelligent transportation [2].

The expeditious growth of the Internet of Vehicles has caused significant hurdles to ample data storage, smart management, and the entire system's information security. The traditional central management approach to handling IoV has problems with real-time response. Blockchain, effective technology for decentralized storage, and decentralized security management has shown significant advantages in embracing bitcoins. In a work by Khan et al. [3], blockchain technology is implemented in vehicle networking applications, especially considering the secure, decentralized storage of big data. They defined different nodes, such as vehicles and road networks, and formed different blockchain subnets. They presented an offshore model of vehicle blockchain data and provided detailed theoretical analysis and numerical results. By leveraging the charging and discharging aptitudes of the Internet of Electric Vehicles (IoEV), demand response can be executed in smart cities to facilitate intelligent energy scheduling and trading. However, IoEV-based systems face several difficulties, such as a deficiency of incentive mechanisms, privacy leakage, and security warnings. This motivated Zhou et al. [4] to exhibit a distributed, privacy-preserved, and incentive-compatible mechanism for IoEV. Mainly, they proposed a consortium blockchain-enabled secure energy-trading structure for electric vehicles with the average expense. A contract-theory-based incentive mechanism is proposed to incentivize more EVs to participate in demand response. Multiple contract details are tailored for the unique features of electric vehicle models. The contract optimization issue befalls into the level of diversity in convex programming and is resolved using the iterative convex–concave system algorithm. Furthermore, they considered the situation where the statistical knowledge of the electric vehicle model is

concealed. In such a case, they demonstrated how to determine the probability distribution of the electric vehicle model by exploring the computational intelligence-based state of charge estimation methods, such as Gaussian process regression. Conclusively, the security and efficiency performance of the proposed scheme is analyzed and validated.

2. System Model

Our proposed system consists of three main contributors. The first is the user or owner of the electric vehicle. The second is the charging station operator, and the third one is the Prosumer. All the participants must make an account on the blockchain network. The membership service provider will provide unique private keys to every user. Electric vehicle information will also be stored on the blockchain. **Figure 3** shows the proposed system model. Power lines are shown with the dotted line, whereas flow lines are shown with connected arrows. The electric vehicle owner can act as a prosumer if they have a renewable energy setup at their premises. They can not only charge their own electric vehicle, but they can also sell it to charging stations. All billing and charging data can be stored over the blockchain using the smart contract. Prosumers can initiate their selling amount through smart contracts, and the one who needs excessive energy at the fixed rate can contact the Prosumer. Smart meters record the amount of energy consumption, and that information can be stored over the blockchain. The Hyperledger fabric-based system allows users to interact independently through blockchain. The operator and producer can also authenticate the registered user and schedule the payment in case of a post-paid charging option. Prosumers can sell excess energy to the charging stations through smart contracts. Charging stations can store all the charging and billing information on the blockchain, which anyone can verify later. Electric vehicle owners can also pay through digital wallets. Payment will be automatically deducted from their wallet according to the charging time and amount through the smart contract.

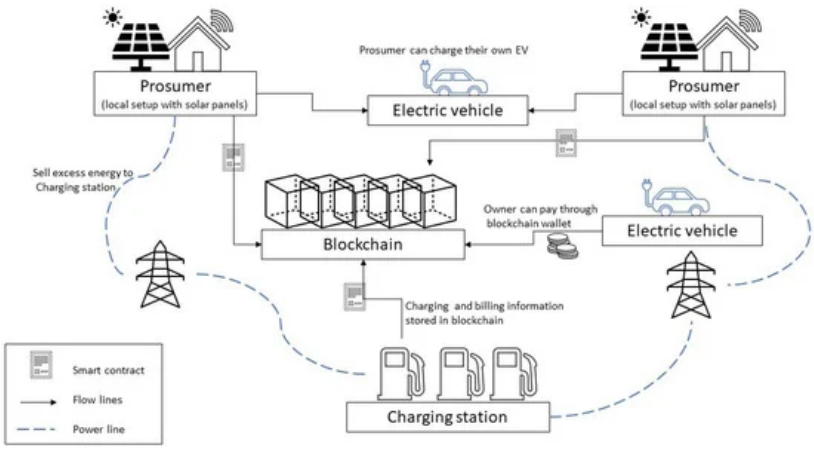

Figure 3. System model of the P2P energy trading and charging system.

3. Smart Contract Process Flow

Hyperledger fabric provides the functionality to write smart contracts. A smart contract is a digital contract between two or more parties. The code written in a smart contract can execute automatically when certain conditions meet. A smart contract is the electronic form of agreement among different participants [5]. Developers create smart contracts to support existing business processes that can manage financial prices or control conditions and represent them as snippets in the JavaScript programming language. In addition, smart contract auditors practice the legal and technical skills needed to translate legal terms into programming languages. Smart contracts can improve the flow of goods or capital, respectively, by ensuring that billing payments are made within a specified time-frame or that funds are released on predetermined terms. Most importantly, smart contract execution is far more efficient than manual business processes [6]. **Figure 4** shows the sequence diagram for the smart charging and payment process flow for peer-to-peer energy trading. If the Prosumer has excessive energy, he can offer this to the charging station through blockchain's smart contract. Suppose the charging stations' owner agrees with the requirements and rates set by the Prosumer. In that case, he can send confirmation through the smart contract. The process of smart payment for electric vehicle charging starts with the initialization of the connection request by the EV owner to the operator. The smart charging station operator forwards the request to the smart contract, which validated the user. After the validation user gets a confirmation notification, and then he requests the producer to transfer energy. After completing the charging process EV owner will get information, and then his system will generate payment requests. He will share the public key with the operator. Finally, the charging station operator will request the producer to make a payment. The producer will transfer the charging amount to the smart contract, whereas

as per the agreement, the smart contract will deduct the amount from the electronic wallet of the EV owner. The smart contract contains the predefined set of codes that automatically executes when a certain condition is met [7]. At the end of the transaction, every participant will receive a notification of success.

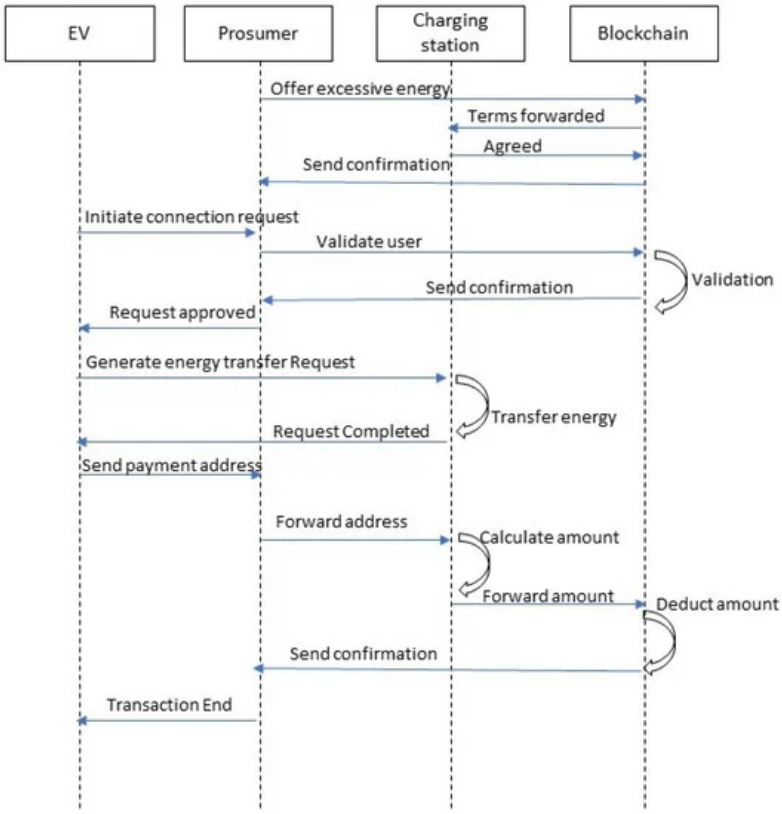

Figure 4. Process Flow diagram for Smart Contract.

4. Consensus Mechanism

In the blockchain, every transaction is confirmed before recording it into the chain. The process of achieving agreement on the correctness of a transaction is called consensus. It assures that no malicious transaction can become a part of the blockchain [8]. Consensus also helps in achieving reliability in the vast network, which involves multiple nodes. Hyperledger Fabric Network's Consensus is the process by which nodes in the network provide a foolproof sequence of transactions and validate which blocks of transactions must adhere to the ledger. All transactions in the proposed block must be validated by consensus according to the guarantee and consensus policy. It is also necessary to agree on the arrangement, accuracy, and implementation results. The consensus is based on a layer of smart contracts to validate the set of required transactions in the block. Consensus in permissioned blockchain depends upon three types of nodes or peers: endorsement nodes, orderers, and committer peers. The client initiates a transaction and sends it to the endorsement nodes. These nodes simulate and execute the transaction; they also sign the endorsed transactions. After receiving the endorsed transaction, the client forwards it to the orderers that verify the endorsement and read-set. If they find it correct, they apply a write-set to it and send it to the committer peer. Finally, the committer peer commits the transition.

5. Overcoming the Oracle Problem

The oracle manages the interaction between blockchain and the real world; it is essential to address the oracle issue to evaluate the effectiveness of blockchain instability issues [9]. The Oracle issue has been described as a security, reliability, and trust dispute between third-party oracle and unreliable blockchain implementation. This can be prevented by using smart contracts and fabric certification [10]. **Figure 5** shows the relationships between the oracle, blockchain, and the certification authority. In a permissioned blockchain, each user has their own unique identity, so Human Oracles can easily be identified. App Oracles can be resolved using smart contracts. Hardware oracle implementation can be solved with Fabric authority. Hardware requested by the customer, such as implementing IoT devices on the blockchain, is authorized by an authorized authority to upload only trusted information to the blockchain.

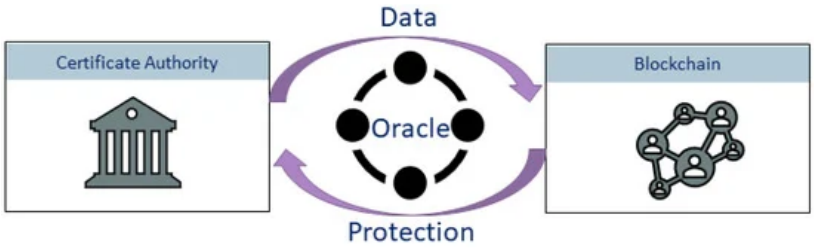

Figure 5. Use of certification authority for overcoming the oracle problem.

6. Blockchain Security

Blockchain is considered a secure platform; however, researchers have identified some prospective issues and presented their solutions. Leng et al. [11] performed a survey to cover the techniques and research directions for blockchain security. The blockchain-based application experiences different kinds of frauds, including objective fraud, subjective fraud, and rating fraud. Therefore, it is needed to enhance the robustness of fraud detection. Feng et al. [12] presented cyber insurance and cyber-risk management approaches to neutralize cyberattacks on the blockchain service network. Data protection in the blockchain can be described by integrity, confidentiality, and availability. It can be improved by applying retrieval techniques on encrypted blockchain data [13] and signature schemes in blockchain [14].

References

1. Perez-Diaz, A.; Gerding, E.; McGroarty, F. Coordination and payment mechanisms for electric vehicle aggregators. App l. Energy 2018, 212, 185–195.
2. Hu, W.; Hu, Y.; Yao, W.; Li, H. A blockchain-based Byzantine consensus algorithm for information authentication of the I nternet of vehicles. IEEE Access 2019, 7, 139703–139711.
3. Khan, P.W.; Byun, Y.C. Secure transactions management using blockchain as a service software for the internet of thin gs. In Software Engineering in IoT, Big Data, Cloud and Mobile Computing; Springer: Berlin/Heidelberg, Germany, 202 1; pp. 117–128.
4. Zhou, Z.; Wang, B.; Guo, Y.; Zhang, Y. Blockchain and computational intelligence inspired incentive-compatible deman d response in Internet of electric vehicles. IEEE Trans. Emerg. Top. Comput. Intell. 2019, 3, 205–216.
5. Khan, P.W.; Byun, Y. A Blockchain-Based Secure Image Encryption Scheme for the Industrial Internet of Things. Entrop y 2020, 22, 175.
6. Fabric, H. Developing Applications. 2021. Available online: https://Hyperledger-fabric.readthedocs.io/en/release-2.2/dev elopapps/developing_applications.html (accessed on 25 March 2021).
7. Shahbazi, Z.; Byun, Y.C. Improving Transactional Data System Based on an Edge Computing–Blockchain–Machine Le arning Integrated Framework. Processes 2021, 9, 92.
8. Xu, G.; Liu, Y.; Khan, P.W. Improvement of the DPoS consensus mechanism in Blockchain based on vague sets. IEEE Trans. Ind. Informatics 2019, 16, 4252–4259.
9. Caldarelli, G. Real-world blockchain applications under the lens of the oracle problem. A systematic literature review. In Proceedings of the 2020 IEEE International Conference on Technology Management, Operations and Decisions (ICTM OD), Marrakech, Morocco, 24–27 November 2020; pp. 1–6.
10. Caldarelli, G.; Rossignoli, C.; Zardini, A. Overcoming the Blockchain Oracle Problem in the Traceability of Non-Fungible Products. Sustainability 2020, 12, 2391.
11. Leng, J.; Zhou, M.; Zhao, L.J.; Huang, Y.; Bian, Y. Blockchain security: A survey of techniques and research directions. I n IEEE Transactions on Services Computing; IEEE: Piscataway, NJ, USA, 2020.
12. Feng, S.; Wang, W.; Xiong, Z.; Niyato, D.; Wang, P.; Wang, S.S. On cyber risk management of blockchain networks: A game theoretic approach. arXiv 2018, arXiv:1804.10412.
13. Tosh, D.K.; Shetty, S.; Liang, X.; Kamhoua, C.A.; Kwiat, K.A.; Njilla, L. Security implications of blockchain cloud with an alysis of block withholding attack. In Proceedings of the 2017 17th IEEE/ACM International Symposium on Cluster, Clo ud and Grid Computing (CCGRID), Madrid, Spain, 14–17 May 2017; pp. 458–467.
14. Sahai, A.; Waters, B. Fuzzy identity-based encryption. In Annual International Conference on the Theory and Applicatio ns of Cryptographic Techniques; Springer: Berlin/Heidelberg, Germany, 2005; pp. 457–473.