Blockchain Privacy and Scalability

Subjects: Computer Science, Interdisciplinary Applications
Contributor: Johann Westphall, Jean Everson Martina

Lower renewable energy generator prices are leading people to install solar panels to reduce their electricity bills or, in some cases, even sell the surplus generated energy to the grid and earn credits from the grid operator. Generally, they are limited to trading the energy they generate with the grid company, which has a dominant role in price determination. Decentralized energy markets might increase both market competitiveness and incentive to further people's adoption of renewable energy, reducing security vulnerabilities and improving resiliency. Blockchain is a widely studied technology to provide decentralization for energy markets. Scalability, privacy, market design, and user security are some of the open research topics.

Keywords: energy ; blockchain ; performance

1. Introduction

Blockchain is a technology that enables a decentralized database in a Peer-to-Peer (P2P) context. It is widely known because of the Bitcoin cryptocurrency [1], and its structure is secure against tampering. Blockchain allows secure transactions between nodes without a TTP (Trusted Third-Party). It is considered to have the potential to enhance the role of consumers in the energy trading system by increasing security and reducing costs [2].

In most energy distribution systems, residences with renewable energy sources can only sell their excess produced energy to the utility company, which impedes broader price negotiation with multiple bidders. Researchers have explored blockchain as an enabler of a decentralized energy trading market, where residences could trade electricity with each other. These residence owners that buy and sell energy are called prosumers.

Beyond energy system improvement, the growth in renewable energy production brings environmental benefits. Considering the mentioned advantages and that blockchain is seen as a possible tool for achieving a decentralized energy market in a microgrid, research on the theme can lead to firmer conclusions on the viability of coupling blockchain with energy markets.

The authors of [3] surveyed blockchain-based energy projects. Even though they recognized the potential of utilizing blockchain to trade energy, they also found that the existing schemes were scarcely documented. The authors argued that future work must provide scientific depth to provide a convincing argument for utilizing blockchain in the energy system.

For [4], the blockchain enhances the energy internet's different layers, but such a network requires privacy protections due to the risk of an attacker acquiring access to consumer behavior characteristics. The distributed ledger also strengthens the guarantee of the metrology devices and their certification, as the network can monitor changes to prevent tampering. Overall, the authors identify the demand for a multilevel approach for blockchains applied to the energy internet.

There are still open research topics on blockchain energy trading schemes in terms of system design, privacy methods to protect user data, and scalable solutions to deal with the amount of data collected through smart meters [2]. The authors of [5] argue that consumers might resist blockchain use in the energy markets due to a lack of privacy and that this context requires a blockchain with low latency and delay. These topics must be addressed to bring this type of system closer to adoption.

2. Blockchains

Blockchains are distributed ledgers, usually without a central authority, with a tamper-resistant and tamper-evident structure [6], enabled through public-key cryptography. This technology became well known for being part of the Bitcoin currency. A header and a data segment form each block. The transaction list is part of the data segment, while the block's cryptographic hash, the previous block's cryptographic hash reference, and a timestamp are parts of the header segment.

A nonce is not always essential but depends on the consensus mechanism. Each transaction performed by a node is digitally signed and can be verified by all nodes using the public key.

There are two main categories of blockchain: permissionless and permissioned. Permissionless blockchains allow anyone to join the network, reading and writing to the ledger as desired. Permissionless blockchains are usually open source. Their consensus rewards publishing protocol-conforming blocks and requires some expense—work or stake—to validate blocks. These consensus constraints exist in permissionless blockchains due to the participation of unknown users who might act maliciously without possible accountability [6].

Permissioned blockchains have restrictions on who can take specific actions in the network. The level of restrictions can vary according to the permissioned blockchain policy. The ledger might be public for reading, but it may have access control for transacting. These settings depend on the context where the network is applied. With known users, the network consensus algorithm can be lighter than permissionless ledgers [6].

3. Hyperledger Fabric, a Permissioned Blockchain That Fits Energy Markets

In scenarios involving players with different roles and privileges, permissioned blockchains provide an extra security layer through access control [7]. Many permissioned blockchain tools differ on privacy level, and in terms of performance, programming language support, and architecture.

Hyperledger Fabric is an enterprise-grade permissioned blockchain that supports smart contracts in general-purpose programming languages [8]. All participants in the network are known, and they belong to an Organization which generates credentials through their CAs (Certificate Authorities).

Each Hyperledger Fabric transaction has to be endorsed by a set of peers responsible for storing ledgers and smart contracts. After that, the orderers receive the transactions and come to a consensus on their order, ensuring that all peers will store all transactions in the same sequence. When receiving the list of ordered transactions in a block, the peers judge the transactions' validity. This transaction flow is called *execute–order–validate* [8].

Smart contracts can distinguish callers' roles by reading their credential fields and, consequentially, applications can be developed with the assurance that the network will follow access control policies. At the same time, Hyperledger Fabric supports pseudo-anonymity through identity mixing algorithms using ZKP (Zero-Knowledge Proof), allowing participants to transact in the network with a certain degree of anonymity.

4. SmartData and Blockchains

SmartData is a standardized high-level Application Programming Interface (API) that facilitates IoT-related application development. It gathers a set of relevant attributes regarding data measured by sensors, including the unit, spatial location, timestamp, and reliability [9]. Blockchains receiving data from sensors may benefit from a standardized format, since it helps data interpretation. Smart contracts can be configured to act according to SmartData's semantics.

Listing 1 demonstrates how SmartData is represented in JavaScript Object Notation (JSON) format. The field **version** determines if the device is stationary, in version "1.1", or moving, version "1.2". The metric is sensed by the device of identification **dev** and has a **value** related to a **unit**. An **uncertainty** degree about the data might be declared. The coordinates **x**, **y**, and **z** express the absolute spatial location associated with a specific instant represented by timestamp **t**. **Version** "1.2" also supports the SmartData cryptographic **signature** [10].

Listing1. Smart Data fields.

{ "version": unsigned char

"unit": unsigned long

"value": double

"uncertainty": unsigned long

"x": long

"y": long

“z”: long

“t”: unsigned long long

“dev”: unsigned long

“signature”: string }

References

1. Rahouti, M.; Xiong, K.; Ghani, N. Bitcoin Concepts, Threats, and Machine-Learning Security Solutions. IEEE Access 2018, 6, 67189–67205.
2. Wang, N.; Zhou, X.; Lu, X.; Guan, Z.; Wu, L.; Du, X.; Guizani, M. When Energy Trading Meets Blockchain in Electrical Power System: The State of the Art. Appl. Sci. 2019, 9, 1561.
3. Johanning, S.; Bruckner, T. Blockchain-based Peer-to-Peer Energy Trade: A Critical Review of Disruptive Potential. In Proceedings of the 2019 16th International Conference on the European Energy Market (EEM), Ljubljana, Slovenia, 18–20 September 2019; pp. 1–8.
4. Zeng, Z.; Li, Y.; Cao, Y.; Zhao, Y.; Zhong, J.; Sidorov, D.; Zeng, X. Blockchain Technology for Information Security of the Energy Internet: Fundamentals, Features, Strategy and Application. Energies 2020, 13, 881.
5. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. 2019, 100, 143–174.
6. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain technology overview. arXiv 2018, arXiv:1906.11078.
7. Dabbagh, M.; Choo, K.K.R.; Beheshti, A.; Tahir, M.; Safa, N.S. A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities. Comput. Secur. 2021, 100, 102078.
8. Team, F.D. A Blockchain Platform for the Enterprise. 2020. Available online: https://hyperledger-fabric.readthedocs.io/en/release-2.3/ (accessed on 1 September 2020).
9. Medeiros Fröhlich, A.A. SmartData: An IoT-ready API for sensor networks. Int. J. Sens. Netw. (IJSNET) 2018, 28, 202–210.
10. LISHA. EPOS 2 User Guide. 2020. Available online: https://epos.lisha.ufsc.br/IoT+Platform#SmartData (accessed on 1 February 2021).