IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 3, March 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203078 |

Secured and Efficient Data Transfer Using Block Chain Technology

K.KALAIMAAMANI, A.ARUN, P.M.JAYASURYA, S.MOHAMED ASHIK, I.MOHAMED IMRAN

Assistant Professor, Department of ECE, Mahendra Engineering College, Mahendhirapuri, Mallasamudram, Namakkal Dt, India

Students, Department of ECE, Mahendra Engineering College, Mahendhirapuri, Mallasamudram, Namakkal Dt, India

ABSTRACT: A DLT-based P2P energy trading system aimed at exploiting the benefits of IOTA Tangle 2.0 and ISCP was shown to only be a fraction of the cost of traditional blockchains for both energy and monetary costs. It achieved this whilst maintaining the inherent benefits provided by DLT and smart contracts of transparency, security and privacy in a completely decentralized manner. The implemented system is also proven to have a significant monetary benefit to participants over wholesale options, with benefits to both prosumers and consumers. The microgrids experienced an average of 166.41% benefit to producers and a 6.3% benefit to consumers in the grid connected scenario per traded. The hierarchical routing infrastructure of interconnected microgrids and the main grid fulfilled the excess energy needs of the system. Additionally, the structure was shown to reduce the overall reliance on the main grid as more entities traded together, increasing benefits to agents in the system.

KEYWORDS: DLT, IOTA, ISCP, DMC, RDC, BLOs, SLOs

I.INTRODUCTION

Internet of things (IOT) has been evolving rapidly in recent years. The number of global Internet of things devices will increase by about 30% to 40% every year and will reach 20.8 million by 2020. In the fields of smart home, intelligent transportation, and industry, an IOT device is used to collect environmental information and send it to a centralized server for further processing or decision making. As more and more IOT devices appear in various versions, especially in critical systems, the need for secure data transfer between devices is increasing. At the same time, in order to realize the communication between numerous devices belonging to different organizations, Internet of things related solutions are seeking effective and reasonable methods and standards [1, 2].

At present, the problems faced by the centralized network architecture of the Internet of things are as follows:(1) if the centralized server fails, the whole network will be paralyzed. A Denial of Service (DOS) attack on a centralized server leads to a single point of failure.(2)Data stored in centralized servers lacks guaranteed accountability and traceability. The centralized system needs to trust a third party for data processing, and the stored data is at risk of deletion or tampering.(3)In the Internet of things, with the exponential growth of the number of Internet of things devices, the centralized server is not efficient in dealing with a large number of end-to-end communications. Therefore, the centralized approach may hinder the development of the Internet of things.

In recent years, people pay more and more attention to blockchain technology. Blockchain is the core supporting technology represented by digital cryptocurrency [3, 4]. Blockchain technology has been applied to fields such as government, medical treatment, copyright, Internet of things, company management, Internet of vehicles, and so on and has promoted many business models that could not be realized previously. The so-called blockchain is a storage method for distributing data, which includes new data usage modes such as point-to-point data transfer, negotiation mechanisms, and encryption algorithms. It is a mode of data exchange by centralizing data and establishing corresponding database. During blockchain data transmission, data needs to be encrypted. Due to the old technology and easy decoding, the original encryption method often leads to the loss of data.

Therefore, homomorphic encryption is used for data protection, which can detect and correct the data while encrypting to ensure the integrity of the data. Complete homomorphic encryption is a special method of encryption. Compared to the general homomorphic encryption algorithm, complete homomorphic encryption allows other people to receive encrypted data and perform any complex operation on the data without a decryption key. The whole process of

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203078 |

computing can be entrusted to others. For example, the whole process of data encryption can not only reduce the cost of data access to others, but also transfer the whole process of computing to others. For example, the whole process of computing can be entrusted to others, which can reduce the cost of data encryption and so on. The data information on the blockchain is encrypted into ciphertext with homomorphic encryption algorithm. The smart contract on the blockchain can process ciphertext without knowing the plaintext information, which significantly improves the security of user data privacy.

II.RELATED WORKS

In order to reach an agreement between decentralized blockchain nodes, all transaction logs in the blockchain must be disclosed to all nodes, which will greatly increase the risk of privacy breaches [7]. In the case of the use of cryptocurrency, analysts can analyze the transaction log to obtain the user's transaction style, as well as the user's personal information and location information [8]. We offer a reliable, personal OTT platform that handles the transaction process with a smart contract that is reliable and configurable. Smart contracts can be predefined for each product on a digital media content website (DMC) within the platform. After negotiating using a smart contract, a real data contract (RDC) is created and issued through a smart contract. A content producer or service provider can easily implement a trading strategy under a predefined smart contract [9].
In the industrial Internet of things (IOT), energy transactions of decentralized nodes occur in various scenarios, such as microgrid, energy collection network, and vehicle to grid network. The alliance blockchain solves the common security and privacy problems caused by the untrusted and opaque energy market [10]. Huang J. and others proposed a new automatic food trading system based on alliance blockchain to improve trust and security in trading. It protects the privacy of stakeholders in the blockchain by using different authentication technologies [11]. Kumar S. S. and others realize the security and privacy protection of data sharing in electronic health system through alliance blockchain [12]. Thirukrishna. J. T. and others proposed CAIPY ecosystem based on smart contract to solve the cumbersome process problems in the field of insurance, which makes automobile insurance simple and transparent. CAIPY shows how smart contracts can support insurance companies without introducing new risks. Smart contracts have great potential to simplify these processes, thereby reducing costs [13].

Liu H. et al. adopted the smart contract technology based on Ethereum platform, established a hierarchical intelligent power distribution trading platform architecture for real-time transaction request and data acquisition, and realized the data security interaction under the high coupling of energy flow and information flow [14]. The combination of homomorphic encryption and Ethereum's smart contract technology makes it possible for insurance companies to obtain a customer's simple EHR text and claim object ID and decide whether to settle a claim even if patient information is not available, strengthening the confidentiality of any confidential information and user information disclosed to unauthorized users during interactions [15].

Based on this study, this paper suggests a reliable way to transfer data to a blockchain based on homomorphic encryption. In view of the problem of exposing data privacy in blockchain, taking user transactions as an example, this research is based on the fully homomorphic encryption algorithm without bootstrap conversion, combined with zero knowledge proof technology, under the account model, proposes the equal and full amount blockchain transaction protocol based on fully homomorphic encryption, and constructs a fully homomorphic encrypted data privacy blockchain based on intelligent contract. It can completely hide the input and output of the traditional blockchain trading system and the transaction details. Except for the transaction parties, the hidden details are completely invisible to anyone else. The threat that the transaction data information on the blockchain is analyzed by other malicious opponents will be greatly reduced, which significantly expands the application scenario of the blockchain.

III.METHODS

Blockchain consists of blocks containing transaction details. This information may be a transfer of cryptocurrency or other data exchange. Each block is logically divided into two parts: block header and block body. Each block is logically divided into two parts: the block head and the block body. Each block header contains the hash value of the previous block and other fields. Therefore, the blocks are connected in a similar way to the linked list as shown in Figure 1. Transaction information is stored in the block body. The first block in the blockchain is called the “genesis” block. The block hash value is obtained by a cryptographic hash, and each block stores the hash of the previous block, which helps keep the content in the blockchain unchanged. If hackers try to change the content of the previous blocks, the original hash value will be invalid. Hash values for subsequent blocks will be invalidated due to the domino effect.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203078 |

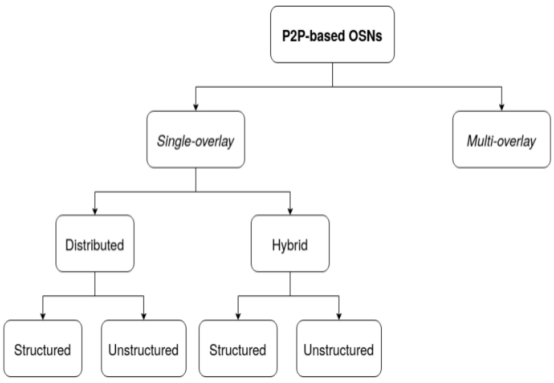

Fig 1: **DATAFLOW DIAGRAM**

This causes more unpredictable fluctuations in time, increasing the burden on the capabilities of the smart meter to predict energy consumption and production for variable time periods. Ethereum gas fees also increase with the traffic on the blockchain, whilst our proposed system has fixed costs. This leads to increased costs as we scale to larger numbers of participants further widening the already huge difference in cost between the two systems. This is also likely to lead to cases where the cost of energy traded in the P2P transactions is less than the gas fee needed to bid for said energy.

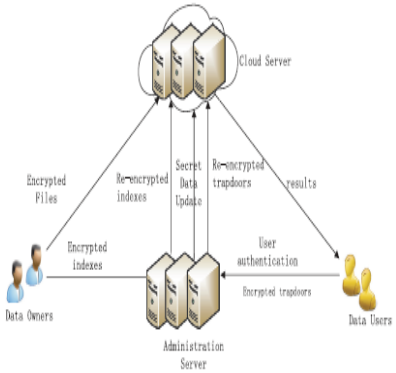

Fig 2: **SYSTEM ARCHITECTURE**

The system was setup off-ledger using the same smart contracts to maintain functionality. Off-ledger simulation was implemented to obtain the results of the mechanism for the entire week period provided by the data set in a timely manner. In this section, we define benefit as the beneficial difference in price agents in the system experience over wholesale alternatives Pgb and Pgs determined to be fixed at 18.9p/kWh [38] and 3.2p/kWh [39] respectively for the week period

Our trading strategy implements a uniform price doubleauction for the market mechanism to match multiple buyers and sellers. This is because it allows the microgrid to act as a single bidding entity when connecting to other grids. The double-auction executes as follows. 1) Place Bids: Bids are placed in the form of buy limit orders (BLOs) submitted by consumers and sell limit orders (SLOs) submitted by producers to conform to the doubleauction market mechanism. The quantity for the bids qi is determined by the energy requirement of the peer δ(M i) defined previously.

IV.RESULTS AND DISCUSSION

The P2P energy trading mechanism is evaluated for both the success as a Layer-2 DLT framework and the benefit of the trading mechanism when applied to an interconnected microgrid system. The system has been implemented on a testbed to prove the functionality over the chosen DLT as well as to obtain metrics from its execution. The smart contracts have been simulated off-ledger to assess the benefit of the market mechanism. In both cases, the system uses real-world data and a python script to model the smart meter prediction capability of production and consumption. We use the script to model the behaviour of each agent in each microgrid when placing bids.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203078 |

Using the methodology from the IOTA Foundation to measure the energy consumption of a GoShimmer network [35], we were able to obtain the energy cost per transaction using a Ruideng UM25C energy meter. Through logging the events of the Wasp chain, we averaged the length of time it took for a bid transaction to be confirmed on the DLT. We benchmark against an Ethereum network. With regards to the Ethereum network, the energy cost per transaction and the time taken per transaction are determined through qualitative research [36], [37]. The Cost per bid is calculated by deploying an identical uniform double-auction smart contract written in solidity to the Remix IDE, and an average gas fee per bid is calculated

By running the private Wasp chains in parallel, the execution time of each microgrid is independent of others. On the other hand, Ethereumblockchain's transaction time depends on how busy the network is. This causes more unpredictable fluctuations in time, increasing the burden on the capabilities of the smart meter to predict energy consumption and production for variable time periods. Ethereum gas fees also increase with the traffic on the blockchain, whilst our proposed system has fixed costs. This leads to increased costs as we scale to larger numbers of participants further widening the already huge difference in cost between the two systems. This is also likely to lead to cases where the cost of energy traded in the P2P transactions is less than the gas fee needed to bid for said energy.

V.CONCLUSION

Blockchain, which is the most well-known type of distributed ledger technology (DLT), has been identified as the key to facilitating P2P energy trading due to the inherent features of decentralization, resilience, privacy and security [4]. However, conventional blockchain technologies still face challenges when applied to a P2P energy trading use case. DLTs based on a directed acyclic graph (DAG) structure overcome many limitations associated with blockchains and have been investigated from the perspective of blockchain replacement in energy management systems. The proposed energy trading system, which is a manifestation of a cyber-physical system (CPS), exploits the benefits brought by IOTA's unique ledger structure as well as the recently introduced IOTA smart contract protocol (ISCP). Further, it implements a uniform double-auction market mechanism and a hierarchical routing structure for interconnected microgrids. Performance evaluation demonstrates key benefits over wholesale markets as well as speed, energy efficiency and cost benefits over conventional blockchain-based P2P energy trading systems

REFERENCES

[1] R. Arumugam and T. Subbaiyan, "A review of dynamic pricing and peer-to-peer energy trading in smart cities with emphasize on electric vehicles," pp. 1–6, 6 2022.
[2]M. Jabbar et al., "A low-cost, open-source peer-to-peer energy trading system for a remote community using the internet-of-things, blockchain, and hypertext transfer protocol," Energies 2022, Vol. 15, Page 4862, vol. 15, p. 4862, 7 2022.
[3]M. K. Thukral, "Emergence of blockchain-technology application in peer-to-peer electrical-energy trading: a review," Clean Energy, vol. 5, pp. 104–123, 3 2021.
[4] J. Abdella et al., "An architecture and performance evaluation of blockchain-based peer-to-peer energy trading," IEEE Transactions on Smart Grid, vol. 12, pp. 3364–3378, 7 2021.
[5]Tushar et al., "Peer-to-Peer Trading in Electricity Networks: An Overview," IEEE Transactions on Smart Grid, vol. 11, no. 4, pp. 3185– 3200, 2020.
[6]A. Ahl, M. Yarime, K. Tanaka, and D. Sagawa, "Review of blockchainbased distributed energy: Implications for institutional development," Renewable and Sustainable Energy Reviews, vol. 107, pp. 200–211, 6 2019.
[7] Z. Guan et al., "Effect: an efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid," Science China Information Sciences 2019 62:3, vol. 62, pp. 1–14, 1 2019. [Online]. Available: https://link.springer.com/article/10.1007/s11432-018-9451-y
[8] T. Sousa et al., "Peer-to-peer and community-based markets: A comprehensive review," Renewable and Sustainable Energy Reviews, vol. 104, pp. 367–378, 4 2019.
[9] N. Wang et al., "When energy trading meets blockchain in electrical power system: The state of the art" Applied Sciences 2019, Vol. 9, Page 1561, vol. 9, p. 1561, 4 2019.
[10]M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security" Proceedings - 2017 Resilience Week, RWS 2017, pp. 18–23, 10 2017.
[11] K. Shuaib, J. A. Abdella, F. Sallabi, and M. Abdel-Hafez, "Using blockchains to secure distributed energy exchange," 2018 5th International Conference on Control, Decision and Information Technologies, CoDIT 2018, pp. 622–627, 6 2018.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203078 |

[12] J. Hwang et al., "Energy prosumer business model using blockchain system to ensure transparency and safety" Energy Procedia, vol. 141, pp. 194–198, 12 2017.[18] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams" IEEE Transactions on Dependable and Secure Computing, vol. 15, pp. 840–852, 9 2018.
[13] C. Zhang et al., "Peer-to-Peer energy trading in a Microgrid," Applied Energy, vol. 220, pp. 1–12, 2018.[Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306261918303398
[14] D. Gregoratti and J. Matamoros, "Distributed energy trading: The multiple-microgrid case," IEEE Transactions on Industrial Electronics, vol. 62, pp. 2551–2559, 2015.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details