PhD Forum 2022 – On-chain Off-chain Blockchain Model for IoT using IPFS

Pooja Khobragade Department of computer science and engineering NIT Rourkela, India
Guide: Ashok Kumar Turuk dept. computer science and engineering NIT Rourkela, India

***Abstract*—Blockchain has become the most revolutionary and trending technology since 2008 with the development of Bitcoin. Besides bitcoin, blockchain can be applied in different sectors, such as finance, healthcare, IoT, security, etc. Blockchain and IoT are two new emerging technologies. IoT has become an integral part of human digital life with the exponential growth of digitally connected devices to the internet. With the development of connected devices, data communication has also increased. Till now, IoT data management has been based on a centralized server. Blockchain technology can protect IoT devices against malicious attacks and single-point failure. This study analyzes the integration of blockchain technology with IoT and also discusses the advantages, challenges in integration, and associated cyber security threats. Also, it provides an architecture for blockchain-enabled secure IoT devices with the Interplanetary File System(IPFS).**

***Index Terms*—Blockchain, IPFS, Security, IoT, Authentication, Smart contract.**

I. Introduction

Blockchain is an emerging technology that gained popularity with its first application in Bitcoin. It is a decentralized, distributed, tamper-proof technology. The problem of the centralized system, such as single points of failure and data integrity, can be overcome by Blockchain [1]. It provides a trusted environment for participants. Peers in blockchain share information over the network Blockchain is distributed digital ledger of cryptographically signed transactions grouped to make a chain-like structure [2]. Transactions are stored in chronological order with a time stamp assigned to each block. Transactions are continuously growing, and new blocks are added to the blockchain, with the consensus of other block nodes. A Block consists of a block header, previous block hash, timestamp, and transaction data. Figure.1 shows the structure of a block in the blockchain.

The Internet of things (IoT) is a network of living and nonliving things that are sensors, actuators, software, and technologies to share data and establish communication over the internet. It is expected that IoT global market will reach one trillion dollars by 2022 [3]. IoT benefits different sectors, such as manufacturing, automotive, agriculture, healthcare, the public sector, etc. IoT devices are prone to cyber-attacks. It is important to secure the IoT network and authenticate the network devices. This work focuses on applying blockchain to IoT nodes to make a secure, immutable, distributed ledger of communication. Also, to use the IPFS system to overcome the data storage problem associated with blockchain.

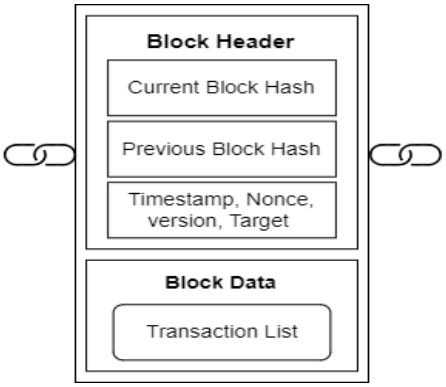

Fig. 1. Block structure

II. Related work and contribution

The centralized system is antiquated because of several issues, such as trust, single-point failure, people and industry shifting towards decentralized system. A decentralized network provides benefits over single-point failure. But the, shortcomings like privacy, security, and unauthorized access control need to be addressed. Authors in [4] used consensus algorithm to authenticate IoT devices. They have proposed blockchain registries to store the device's identity. In [5], security requirements of all layer of IoT is listed and have used blockchain to achieve security. Author in [6] proposed a smart contract-enabled blockchain authentication mechanism and have introduced off-chain storing of data via fog node. A distributed off-chain data storage using IPFS to achieve consistency, integrity, and data availability is proposed in [7]. A framework for message handling in VEN network using IPFS and AI is proposed in [8]also proposed three-layer system message layer, storage layer, and Blockchain layer, RSU is used for communication, and Certification authority is used for device registration, using proposed layer architecture get an 80-85% reduced storage overhead, and 15-18% reduced computation overhead. Author in [9], used proxy re-encryption method to achieve data security, privacy, and confidentiality. To deal with the storage problem authors have used the Ethereum blockchain network with IPFS. A smart contract-based blockchain authentication for smart farming is proposed by [10]. Authentication is done in two phases, device-to-device and device-to-gateway, and the PBFT consensus algorithm is used to validate and add blocks to the network. To reduce network cost in [11] proposed a location-based authentication.

The mutual authentication is done without any registration center authority (RAC) or gateway node to reduce. Table I summarized the blockchain-based IoT authentication schemes reported in the literature.

The contribution of the paper is summarized as below:

- Study of Integration issue of blockchain with IoT.
- Proposed distributed decentralized on-chain off-chain blockchain IPFS model for IoT security.
- Design an authentication scheme for IoT devices.

III. Blockchain for Internet of Things(IoT)

IoT contains resource-constraint devices that are capable of establishing communication without human involvement. As IoT technology is a widely successful and promising technology, it suffers from many issues like security, single point failure, data privacy, low storage capacity, low Interoperability, lack of data analysis, and high-cost [16] [17]. Figure 2 shows the advantages of applying blockchain in IoT.

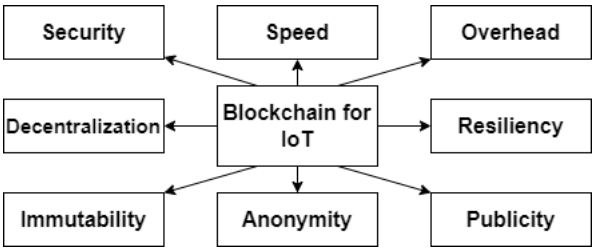

Fig. 2. Advantage of Blockchain in IoT

Blockchain provides peer-to-peer communication in a distributed network, which shares the cost and storage among peers [18]. Blockchain is an immutable and real-time ledger to store transactions which provides reliability. With a decentralized nature, blockchain solves trust and security issues in a system without the involvement of any third party or centralized authority [19]. To provide privacy, records are time-stamped, encrypted, and digitally signed. Only private key holders have the right to access the record. Blockchain provides a secure socket layer certificate to validate the user and device for strong authentication [20]. The blockchain features like distributed nature, data integrity and security, reliability, decentralized nature, transparency and traceability, cost saving, efficiency, interoperability, and verifiability enable blockchain to overcome the issue in the IoT [21].

However, the application of blockchain in IoT is not very easy several issues like resource requirements, high computation, storage cost, power, scalability, low throughput are present during the integration of blockchain with IoT [22].

A. Research challenges

- Resource-constrained devices are vulnerable to attack. If false or corrupted data enter the chain, it will always reside in the network.
- IoT device because devices are incapable of solving complex puzzles, so consensus protocol needs to apply carefully.
- IoT generates a large amount of data, so there should be a technique to normalize those data.
- Data privacy introduces a complex blockchain structure.

The limitation of IoT needs to be taken care of to apply blockchain effectively in IoT applications [23].

IV. Proposed work

This section consists proposed system model for blockchain-IoT using an Interplanetary File System(IPFS). Blockchain-based on-chain, off-chain model is proposed to solve the storage and scalability issue in integrating blockchain with IoT. An authentication scheme using a smart contract provides security to the system.

A. Components

- **IoT device**: IoT device in this network act as a peer that sends data to the blockchain network.
- **Bockchain**: Hybrid blockchain model is used for communication and data sharing.
- **IPFS**: Interplanetary file system is distributed peer-to-peer data storing, accessing application. IPFS uses content addressing mode to access the data and is compatible with the Ethereum blockchain network.
- **Gateway node**: IoT device continuously collects the data, but not all data contain information, so the gateway node selects the useful data and sends it to the network.
- **User**: User sends the request to the blockchain network to access the data and get access details.

B. Smart contract

Smart contract is a set of immutable instructions called chain code. Smart contracts provide access policy to the nodes of the network. Smart contract is unchangeable once written and automatically executed once the predetermined conditions are met [24].

C. Full node and Light node

Full nodes maintain a record of the full blockchain in storage. Full nodes can participate in the mining process. A full node helps to check data correctness and participate in the consensus process.

Light node does not keep full blockchain. They store only the last updated transaction history. A light node receives a transaction list from a full node [25].

D. Proposed architecture

Using the above components below, architecture is proposed.

TABLE I
LITERATURE SURVEY ON BLOCKCHAIN AUTHENTICATION IN IOT

Author	Goal	Contribution
Dwidedi et al. [6]	Authentication using smart contract	The decentralized system using Ethereum smart contract and IPFS.
Javed et al. [8]	Storage cost and data availability	Blockchain-based data announcement system for vehicular energy network(VEN).
Hasan et al. [9]	Privacy and confidentiality of IoT	Design a decentralized storage system for IoT using IPFS.
Dagher et al. [12]	Access control provision of Blockchain network	Blockchain-based framework to enable efficient, interoperable and secure access to medical records
Hammi et al. [13]	Data integrity management through Blockchain	"Bubble of Trust" to ensure a robust authentication and identification of the device.
Lu et al. [14]	Privacy guarantee through blockchain	Blockchain to empower secure data sharing platform for distributed parties.
Iftekhar et al. [15]	Availability improvement through blockchain	Food tracking infrastructure with the enterprise-ready blockchain platform using Hyperledger fabric.

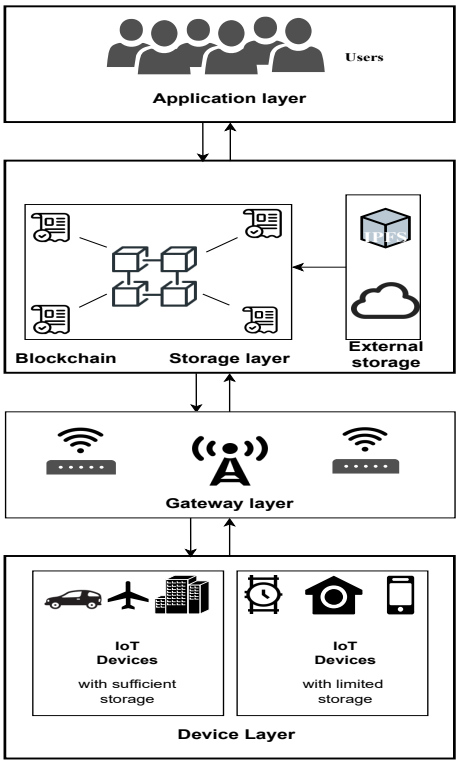

Fig. 3. Proposed 4-layer Architecture for Blockchain-based IoT

V. SYSTEM ARCHITECTURE

A. Device registration

Our proposed solution can apply to any IoT device and does not need any special hardware. Device registration is the initial phase, where the device sends its information to the blockchain network to get paired with it.

B. Gateway registration

Gateway device work as a middle layer between IoT devices and the blockchain network. IoT devices send data to the gateway node, and the gateway device sends filtered data to the blockchain network before that gateway device needs to be registered with the blockchain network.

C. Device authentication

Register IoT devices can only be part of the blockchain network. If a device is registered with the blockchain network, it starts communication with the blockchain network.

D. Data storage

Data storage can be done with two types: directly storing full data to the blockchain network or storing on IPFS, where part of the data is stored in the blockchain network.

E. Incentive mechanism

Each IoT device is one node in the blockchain network that participates in the mining process and consensus to become the next publisher of the block. The incentive process helps to preserve security and trust between nodes by getting rewards for correct mining and penalties for incorrect data or malicious activity.

All the registration and authentication of the device can be done with the help of a smart contract. Smart contracts are separately constructed for each registration and authentication process.

F. Attack associated with Blockchain IoT integration

- **Sybli attack:** In a peer-to-peer network sybli attacker node use multiple fake identities to send the wrong information. This type of attack aims to undermine the authority or power in a reputable system by gaining the majority of influence in the network.
- **Spoofing attack:** In a spoofing attack attacker steals the identity of the valid user to gain the privilege of a legitimate user.
- **Message substitution attack:** Attacker alters the original message during its transit in such a way that the receiver accepts the forged message.
- **Denial of service attack:** Attacker prevents the legitimate user access to the network. DoS attack can be performed in two types(1) By flooding the target. (2) By exploitation of protocol flaw.

- **Message reply attack:** Successful message verification does not contain a time stamp. The attacker records the selective message and replays them without modification.

VI. Design Requirement

A. Elliptic curve Cryptography

Elliptic curve cryptography(ECC) is a type of asymmetric key encryption. An elliptic curve is a special type of polynomial equation that is used for cryptography operations. ECC uses here for selecting key pairs of public key and private key and performs the encryption and decryption method. ECC is a fundamentally different approach than RSA. ECC is based on one-way property. It is easy to perform calculations but infeasible to revert the result of a calculation equation.1 shows the Elliptic curve polynomial equation.

$$y^2 = x^3 + a.x + b \tag{1}$$

B. smart contract design

Smart contract is written in a high-level language, like solidity or python for Ethereum. Smart contracts are compiled into bytecode using a solidity compiler. Any blockchain user can trigger the function and smart contract executed. Figure.4shows the structure of smart contract.

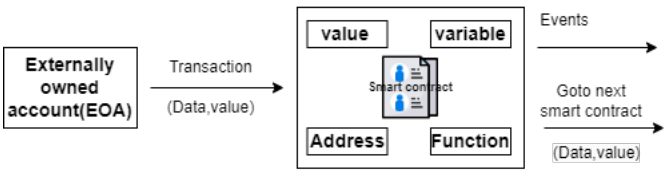

Fig. 4. Smart contract structure [24]

VII. Flow chart

This section shows the flow diagram of the proposed system. IoT device authentication is done with the help of a smart contract. If the IoT device is authorized, then start data collection. Data preprocessing is done, and data is stored in blockchain or IPFS.

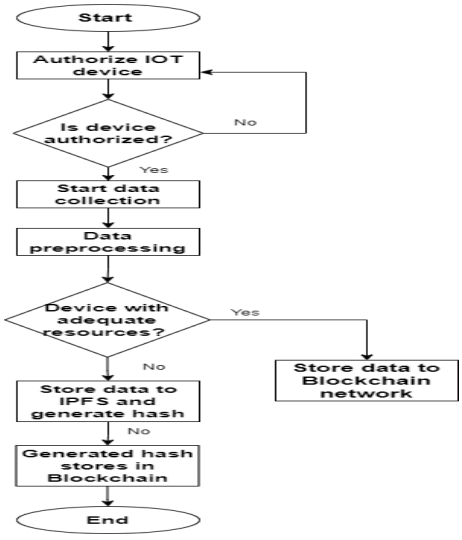

Fig. 5. flow chart of proposed model

VIII. Conclusion

Beyond cryptocurrency, blockchain has many different applications. Blockchain technology is becoming increasingly popular as a key technology for the future, with both businesses and governments exploring its potential to improve services. Our proposed work focuses on the application of blockchain to provide security and storage solutions for IoT applications. Blockchain and IPFS can be used together to create decentralized applications. We plan to design a system model that provides security by authentication of IoT devices via smart contracts and allow devices to become part of the blockchain network. Storage issues solve by using Interplanetary File System(IPFS) to store data from IoT devices. We also compare our model with existing blockchain based IoT model.

References

[1] A. I. Sanka, M. Irfan, I. Huang, and R. C. Cheung, "A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research," *Computer Communications*, 2021.

[2] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *arXiv preprint arXiv:1906.11078*, 2019.

[3] Y.-J. Choi, H.-J. Kang, and I.-G. Lee, "Scalable and secure internet of things connectivity," *Electronics*, vol. 8, no. 7, p. 752, 2019.

[4] M. Mukhandi, F. Damião, J. Granjal, and J. P. Vilela, "Blockchain-based device identity management with consensus authentication for iot devices," in *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 433–436, IEEE, 2022.

[5] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for iot security," *Internet of Things*, vol. 1, pp. 1–13, 2018.

[6] S. K. Dwivedi, R. Amin, and S. Vollala, "Smart contract and ipfs-based trustworthy secure data storage and device authentication scheme in fog computing environment," *Peer-to-Peer Networking and Applications*, pp. 1–21, 2022.

[7] R. Kumar, N. Marchang, and R. Tripathi, "Distributed off-chain storage of patient diagnostic reports in healthcare system using ipfs and blockchain," in *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, pp. 1–5, IEEE, 2020.

[8] M. U. Javed, A. Jamal, E. H. Alkhammash, M. Hadjouni, S. A. Bahaj, and N. Javaid, "Secure message handling in vehicular energy networks using blockchain and artificially intelligent ipfs," *IEEE Access*, vol. 10, pp. 82063–82075, 2022.

[9] H. R. Hasan, K. Salah, I. Yaqoob, R. Jayaraman, S. Pesic, and M. Omar, "Trustworthy iot data streaming using blockchain and ipfs," *IEEE Access*, vol. 10, pp. 17707–17721, 2022.

[10] A. Vangala, A. K. Sutrala, A. K. Das, and M. Jo, "Smart contract-based blockchain-envisioned authentication scheme for smart farming," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10792–10806, 2021.

[11] M. Vivekanandan *et al.*, "Bidapsca5g: Blockchain based internet of things (iot) device to device authentication protocol for smart city applications using 5g technology," *Peer-to-Peer Networking and Applications*, vol. 14, no. 1, pp. 403–419, 2021.

[12] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable cities and society*, vol. 39, pp. 283–297, 2018.

[13] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for iot," *Computers & Security*, vol. 78, pp. 126–142, 2018.

[14] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, 2019.

[15] A. Iftekhar, X. Cui, M. Hassan, and W. Afzal, "Application of blockchain and internet of things to ensure tamper-proof data availability for food safety," *Journal of Food Quality*, vol. 2020, 2020.

[16] M. Hrouga, A. Sbihi, and M. Chavallard, "The potentials of combining blockchain technology and internet of things for digital reverse supply chain: a case study," *Journal of Cleaner Production*, vol. 337, p. 130609, 2022.

[17] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for iot," in *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pp. 173–178, IEEE, 2017.

[18] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain: research and applications*, vol. 3, no. 2, p. 100067, 2022.

[19] A. S. Rajasekaran, M. Azees, and F. Al-Turjman, "A comprehensive survey on blockchain technology," *Sustainable Energy Technologies and Assessments*, vol. 52, p. 102039, 2022.

[20] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the iot and industrial iot: A review," *Internet of Things*, vol. 10, p. 100081, 2020.

[21] K. Azbeg, O. Ouchetto, and S. J. Andaloussi, "Blockmedcare: A healthcare system based on iot, blockchain and ipfs for data management security," *Egyptian Informatics Journal*, vol. 23, no. 2, pp. 329–343, 2022.

[22] S. Qi, Y. Lu, Y. Zheng, Y. Li, and X. Chen, "Cpds: Enabling compressed and private data sharing for industrial internet of things over blockchain," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2376–2387, 2020.

[23] Y. Li, Y. Yu, and X. Wang, "Three-tier storage framework based on tbchain and ipfs for protecting iot security and privacy," *ACM Transactions on Internet Technology (TOIT)*, 2022.

[24] I. Karamitsos, M. Papadaki, N. B. Al Barghuthi, *et al.*, "Design of the blockchain smart contract: A use case for real estate," *Journal of Information Security*, vol. 9, no. 03, p. 177, 2018.

[25] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of iot applications in blockchain systems: Architecture, consensus, and traffic modeling," *ACM Computing Surveys (CSUR)*, vol. 53, no. 1, pp. 1–32, 2020.