Blockchain in IoT-Enabled Smart Home Network Security

Vidyashree K P  
Dept. of Information Science and Engineering  
Vidyavardhaka College of EngineeringMysore  
[@vvce.ac.in](mailto:4vv19is045@vvce.ac.in)

Mohan Prakash V  
Dept. of Information Science and Engineering  
Vidyavardhaka College of EngineeringMysore  
[4vv19is050@vvce.ac.in](mailto:4vv19is050@vvce.ac.in)Manoj M   
Dept. of Information Science and Engineering  
Vidyavardhaka College of EngineeringMysore  
[4vv19is045@vvce.ac.in](mailto:4vv19is045@vvce.ac.in)

Bharath M  
Dept. of Information Science and Engineering  
Vidyavardhaka College of EngineeringMysore  
[4vv19is013@vvce.ac.in](mailto:4vv19is013@vvce.ac.in)Darshan V  
Dept. of Information Science and Engineering  
Vidyavardhaka College of EngineeringMysore  
[4vv19is019@vvce.ac.in](mailto:4vv19is019@vvce.ac.in)

*Abstract*—Network security is a vast topic that combines process devices and technologies. Network security is the group of rules and configurations designed to protect the integrity, confidentiality, and accessibility of devices. The network nowadays has become complex, which is changing the threatened environment. Similarly, smart homes are also becoming prone to security threats. Adopting blockchain-based home automation technology reduces numerous security problems which arise due to equipment’s small power and storage, making people vulnerable to various crime attacks, including ransomware.

Keywords—IoT, Blockchain, Consensus, Consortium, Smart Contracts, Ethereum.

# **1. Introduction**

Recently, IoT devices are used in many sectors of day-to-day life, including Smart homes. Smart home automation is gaining popularity among the current application of the Internet of Things. Sensors are employed within the home via wireless connectivity to be accessible remotely by the homeowners to operate these devices. Due to the vast increase in the smart home IoT devices in the market such as power switches, light bulbs, locks, and many more.

While IoT devices play a huge role in the discussion of IoT security, placing all the focus on this aspect of the IoT does not provide a full picture of why security is necessary and what it entails vulnerabilities, malware, escalated cyberattacks, information theft and unknown exposure, device mismanagement and misconfiguration are a few factors that make IoT security critical today.

Despite the limited computing capacity of most IoT devices, space can still be infected by malware. IoT botnet malware is among the most frequently seen variants. The Mirai botnet has had a major and widespread impact because of poor security and access controls present in many Internet of Things devices. Numerous Mirai versions and Distributed Denial of Service(DDoS) attacks have become more frequent as a result of the public release of its source code in 2016[1]. A real-life instance of illegal hacking in which a perpetrator attempted to obtain data from a North American casino using a fish tank was made public in 2018. Despite the casino having implemented certain security measures to identify the risks, the tank is nevertheless hacked by the hacker so that they could send data to a device in Finland[2].

In order to reduce current problems in centralized network security designs and protect against potential attacks on home automation gateways, propose a blockchain-based home automation gateways network design. The term “Blockchain” refers to a group of distributed ledger technologies that can be programmed to record and track virtually any valuable information, including money transfers, health information, property titles and so forth[3]. The use of blockchain in the smart homes greatly reduces security concerns such as authentication and authorization, confidentiality, integrity and single point of attack.

There are three ways that blockchain is currently being used. The first is public blockchain, also known as the permissionless blockchain, in which the ledger is completely distributed and open to users, miners, developers and community members. The second way uses a private blockchain, which is a permissioned blockchain that may only be accessed by pre-selected members of the known organization[2]. Consortium blockchain technology, which uses both public and private blockchain to implement blockchain, is the third method. In this only a predetermined group of nodes are pledged for block validation[4].

According to[5], the blockchain model is an attractive alternative compared to the centralized conventional IoT model which has significant issues addressing the requirement for security in smart homes. In a centralized IoT model many IoT-based devices are linked together and centered on smart home gateways as explained in [6]. For IoT devices, a decentralized data management system is used with smart contracts used to enforce all data permissions and the blockchain used to store the audit trail of data access. Without the need for centralized system, multiple parties can specify rules to govern their interactions through the use of smart contracts applications, which are independently enforced in the blockchain. In [7], they offer a framework that stores the raw data in the secure platform with a trusted execution environment (TEE) while also storing the hash of the data in the blockchain.

Many blockchain based smart home architecture are designed using Ethereum smart contracts. Ethereum is a public blockchain-based distributed computing platform which has it’s own language such as Solidity and Serpent developers can write and compile using this language [8]. Ethereum can be used to combine computing systems with blockchain.This type of block chain has a difficult process of implementation and scalability is an issue. It also need huge storage and also consumes more energy.

Following is how the remaining sections of this paper is structured: Section 2 examines the background and related work, section 3 outlines the Literature review. Finally the paper is concluded and future work is discussed in section 4.

# **2. Background and related work**

**2.1. Blockchain**

Blockchain is defined as a decentralized and distributed public ledger technology in peer to peer network. It uses a linked block a structure to store and verify the data and creates a tamper-proof digital platform for storing and sharing data by using a consensus mechanism to synchronize changes in data [9]. Each request is recorded in a series of blocks, each of which has a distinct digital certificate for use in verification. Blockchains are the best option for storing sensitive data due to the fact that the ledger is created and maintained by everyone involved in the system equally, eliminating the need for a central controller to oversee operations.

Consensus algorithms are used to keep the same transaction records in all the nodes, which are consisted of the proving work of the transaction and the selecting policy of the block [10]. Few common consensus algorithms are PoW (Proof of Work) and PoS (Proof of Stake). The PoW is a mechanism in which the majority of nodes on the network decide on a single state it is said consensus is achieved. PoS is an alternative to PoW which reflects on the holding assets of the participating nodes.

**2.2.** **Smart Home Network Security**

Smart homes are automated structures with detection and control equipment already installed, including HVAC (heating, ventilation and air conditioning), lighting, hardware and security systems. These contemporary systems sometimes referred to as “gateways”, comprise switches and sensors that interact with the central axis. IoT controls the network connectivity of these control systems, which have user interfaces that communicate with tablets, smartphones and computers. In the world of research, numerous security infrastructures have been proposed. In fact, the majority of these cutting-edge infrastructures are cumbersomely centralized, creating a single point of attack which hinders the scaling and widespread adoption of IoT applications and poses serious privacy and security risks. At this time blockchain stands out as one of the best candidates for creating a secure, distributed/decentralized ecosystem for IoT systems although blockchain has been thoroughly studied in a variety of context, including smart cities and cloud.

**Public Blockchain systems for smart homes**

By fusing the IoT and blockchain the authors of [11] created a smart district model and created user access to the power grid. Users are able to work with the power grid system via blockchain by using da eveloped prototype model. Any person who has a solar panel setup can interact with the network to primarily buy and/or sell energy directly over the blockchain mechanism. This could serve as an important example of how blockchain-based IoT applications implemented and replicated in the real world. This study also demonstrates some important prerequisites for smart home systems that could serve as a significant allusion in the creation of new smart home applications.

A lightweight integrated blockchain (ELIB) paradigm for IoT systems was created by the authors of [12] using a public blockchain, cloud computing and smart contracts. It was then applied in a smart home for performance evaluation. Even though the model speeds up processing and displays appropriate performance, using the cloud could rise system costs. Public permissionless blockchain make use of expensive consensus procedures, such as proof of work (PoW) proof of stack (PoS), or protocols that demand specialized hardware, like proof of elapsed time. In IoT systems where devices are diverse and power constrained, such standards do not apply. The throughput and latency demands of IoT applications, which frequently call for hundreds of transactions to be committed to the ledger within milliseconds to seconds, cannot be met by them either.

**Private Blockchain systems for smart homes**

A Blockchain-based secure and lightweight architecture for a smart home has been presented by writers in [12]. According to the suggested plan, the owner of the smart home oversees the local blockchain from a central location. A shared key generated by the participating nodes is used to protect all communication between the local devices and the overlay nodes. Lightweight hashing was used by the authors to highlight any deviations in the transactions. The suggested architecture guaranteed data availability, confidentiality, and integrity in addition to providing defense against Distributed Denial-of-Service (DDoS) assaults. This architecture makes use of cloud storage to get around the smart home device’s low memory issue.

**Consortium Blockchain systems for smart homes**

A consortium blockchain is used as the distributed ledger to record all IoT devices and their services. It serves as the main channel of communication for IoT services with their users and provides significantly greater performance and scalability and then permission-less public blockchains. The IoT network may decentralize eliminating the centralized servers that are frequently SPOF. Additionally, to protect IoT services from unwanted access, the platform can make use of access control features added by consortium blockchains. Finally, because every modification to IoT services, as well as every service request and answer, is permanently recorded on the ledger, the blockchain effectively functions as a data historian for data audits [13].

To accomplish confidentiality, integrity, scalability, availability and make smart homes safe and secure, the consortium blockchain was integrated with cloud computing and the architecture was presented. The suggested plan utilized green cloud computing and demonstrated how to implement a blockchain in a smart home network to manipulate transactions. The method uses a green broker to manage the suggested model’s choice of energy-efficient service providers in order to minimize the elements affecting the environmental situations and also they describe how to create a data privacy-focused smart home system based on a consortium blockchain. Simulated results of the models performance were reviewed. However, the architecture’s explanation of energy use and activity processing time was lacking.

**3. Literature Review**

The literature survey provides an overview of the current state of research in the field of IoT-enabled smart homes and blockchain technology. The articles and studies reviewed in this section have shed light on the various applications and benefits of incorporating blockchain in smart home systems. These articles have also discussed various security and privacy challenges that need to be addressed while using blockchain technology in smart home systems. The literature survey highlights the various approaches and mechanisms proposed by researchers for addressing these challenges and for improving the security and privacy of smart homes.

In addition, the literature survey has also shown that there is still a lot of scope for further research in this field. Researchers are exploring various avenues for improving the performance and scalability of blockchain-based smart home systems. Additionally, researchers are also investigating new ways to address the security and privacy challenges of smart homes and to develop more efficient and user-friendly smart home systems. The literature survey has thus provided valuable insights into the current state of research in the field of IoT-enabled smart homes and blockchain technology and has identified areas that need further investigation and development.

**Table 1 Relevant studies on advantages and disadvantages of securing smart homes with blockchain**

|  |  |  |  |
| --- | --- | --- | --- |
| Related Studies | Advantages | Disadvantages | Methodology |
| [5] | * Blockchain can improve efficiency and speed, as it can complete time consuming process and automate them, maximizing efficiency * The edge server boosts system scalability by outsourcing labor-intensive processing tasks and aggregating data to the cloud safely and securely via a differential privacy method | * The current industry faces serious transparency problems. The organization made an effort to impose more laws and restrictions. With blockchain, smart homes operate on a fully decentralized network, eliminating the need for centralized control and enhancing system transparency | * Using a attribute based access control system to authenticate users of smart homes and IoT devices allows for realtime communication between home users and a fully validating blockchain node |
| [11] | * An overlay network and cloud storages coordinating data transactions with blockchain to provide security and privacy | * Difficulty of interoperability of different home devices. * Interoperability, the ability to communicate between other devices from different manufacturers represents a crucial condition for the development of smart home | * Blockchain uses a token called as a consensus mechanism, to generate a unique, specific HASH corresponding to the information contained in the block |
| [6] | * Provides the solution to minimize the confidentiality, integrity and authentication issues of the heterogenous IoT and centralized gateways | * Difficulty in Implementation * Scalability issues | * Usage of SHA2 encryption technique to resolve confidentiality and authentication issues * The integrity of the data is kept in the gateway if the architecture |
| [7] | * Decentralized access policy provides data integrity and security | * Scalability issues | * Ethereum is used for evaluate the transaction * Provide a framework that stores the hash of the data in the blockchain and store raw data in secure storage platform using trusted execution environment (TEE) |
| [10] | * Suitable for massive IoT environment scenarios and IoT devices can take advantage of safe and efficient transmission by using the delegated proof of node technique or S-DTS | * Limited number of witness can lead to centralization of network in DPoN | * Delegated proof of node is used to implement blockchain |
| [12] | * ELIB model meets the necessitates of security and privacy | * High energy consumption * Only suitable for few applictaions | * It mainly operates in 3 levels namely consensus algorithm, CC model and DTM scheme * ElIB generates an overlay network where highly equipped resources can merge to a public blockchain which verifies security and privacy |
| [14] | * Provides real-time analysis and monitoring of data * Scalability issue of blockchain is resolved |  | * Used a 3 tier architecture IoT-Fog-cloud for secure and efficient information processing |
| [15] | * Sharing of data without an intermediatory between trusted and non-trusted stake holders | * Since Ethereum is used implementation cost is high | * It uses Ethereum based public blockchain storing the transactions |
| [16] | * The block can be verified and inspected by all nodes, which can help improve trust and access to the data | * High implementation cost * Require private key to access the information stored by the blockchain but the Wallet will be in danger if it doesn’t work | * A modified smart home network is built with the use of consortium blockchain architecture |
| [8] | * Easy synchronization between IoT devices with other devices because of distributed ledger | * Security is compromised due to involvement of third party * Ethereum is not fast enough for some time sensitive domains | * RSA public key cryptosystems are used to manage keys where public key are stored in Ethereum and private keys are stored in individual devices |

##### **4. Conclusion**

This paper introduces the application, existing problems, and solutions for smart homes based on a blockchain architecture. Firstly we found several concerns involved in centralized smart home architecture such as confidentiality, integrity, and Distributed denial of service (DDoS). Blockchain was integrated into this architecture to resolve the issues in the centralized architecture. Secondly, we summarized how public, private, and consortium blockchains are integrated with smart home systems. Further, we discussed the different consensus mechanisms used in the blockchain. We have done a comparative analysis of work done by different researchers in this field and found that issues found in centralized architecture were resolved by distributed systems but a new problem of scalability has arisen in most of the proposed architecture. Further research can be done to resolve the scalability issue present in the distributed architecture.

##### **References**

[1] X. Zhang, O. Upton, N. L. Beebe, and K. K. R. Choo, “IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers,” *Forensic Science International: Digital Investigation*, vol. 32, Apr. 2020, doi: 10.1016/j.fsidi.2020.300926.

[2] S. Arif, M. A. Khan, S. U. Rehman, M. A. Kabir, and M. Imran, “Investigating Smart Home Security: Is Blockchain the Answer?,” *IEEE Access*, vol. 8, pp. 117802–117816, 2020, doi: 10.1109/ACCESS.2020.3004662.

[3] Mohiuddin Ahmed, “Introduction to Blockchain,” 2020. [Online]. Available: https://www.researchgate.net/publication/343601688

[4] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” in *2017 IEEE International Congress on Big Data (BigData Congress)*, Jun. 2017, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.

[5] A. Qashlan, P. Nanda, X. He, and M. Mohanty, “Privacy-Preserving Mechanism in Smart Home Using Blockchain,” *IEEE Access*, vol. 9, pp. 103651–103669, 2021, doi: 10.1109/ACCESS.2021.3098795.

[6] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, “A blockchain-based smart home gateway architecture for preventing data forgery,” *Human-centric Computing and Information Sciences*, vol. 10, no. 1, p. 9, Dec. 2020, doi: 10.1186/s13673-020-0214-5.

[7] G. Ayoade, V. Karande, L. Khan, and K. Hamlen, “Decentralized IoT Data Management Using BlockChain and Trusted Execution Environment,” in *2018 IEEE International Conference on Information Reuse and Integration (IRI)*, Jul. 2018, pp. 15–22. doi: 10.1109/IRI.2018.00011.

[8] S. Huh, S. Cho, and S. Kim, “Managing IoT devices using blockchain platform,” in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 2017, pp. 464–467. doi: 10.23919/ICACT.2017.7890132.

[9] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, “A survey on privacy protection in blockchain system,” *Journal of Network and Computer Applications*, vol. 126, pp. 45–58, Jan. 2019, doi: 10.1016/j.jnca.2018.10.020.

[10] D. Y. Kim, S. D. Min, and S. Kim, “A DPN (delegated proof of node) mechanism for secure data transmission in IoT services,” *Computers, Materials and Continua*, vol. 60, no. 1, pp. 1–14, 2019, doi: 10.32604/cmc.2019.06102.

[11] C. Lazaroiu and M. Roscia, “Smart district through IoT and Blockchain,” in *2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA)*, Nov. 2017, pp. 454–461. doi: 10.1109/ICRERA.2017.8191102.

[12] S. N. Mohanty *et al.*, “An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy,” *Future Generation Computer Systems*, vol. 102, pp. 1027–1037, Jan. 2020, doi: 10.1016/j.future.2019.09.050.

[13] R. Zhang, C. Xu, and M. Xie, “Secure Decentralized IoT Service Platform using Consortium Blockchain,” Sep. 2022, doi: 10.3390/s22218186.

[14] B. Kumar Mohanta, “INTERNET OF THINGS ENABLE SMART HOME SECURITY ISSUE ADDRESS USING BLOCKCHAIN.”

[15] N. R. Pradhan and A. P. Singh, “Smart contracts for automated control system in Blockchain based smart cities,” *J Ambient Intell Smart Environ*, vol. 13, no. 3, pp. 253–267, May 2021, doi: 10.3233/ais-210601.

[16] W. She, Z.-H. Gu, X.-K. Lyu, Q. Liu, Z. Tian, and W. Liu, “Homomorphic Consortium Blockchain for Smart Home System Sensitive Data Privacy Preserving,” *IEEE Access*, vol. 7, pp. 62058–62070, 2019, doi: 10.1109/ACCESS.2019.2916345.