INTERNET OF THINGS SECURITY BASED ON BLOCKCHAIN TECHNOLOGY

Madiyar Seidullayev
Tashkent University of Information Technologies named after
Muhammad al-Khwarizmi
Tashkent, Uzbekistan
mr.madiyar95@gmail.com

Abstract: *Blockchain, a distributed tabulation system, rose to fame as the foundation of the Bitcoin currency. In terms of exploration and operationally successful businesses, it has experienced tremendous expansion throughout the years. Blockchain technology, which is decentralized and uses encryption as its foundation, can elegantly solve the difficult Generals Problem. For applications that require decentralized agreements among untrusted peers without the use of a centralized authority, it is therefore a solid option. The Internet of effects, a technical paradigm in which various little biases, such as detectors, actual bluffs, and RFID tags, are connected by a common dispatching medium, makes it possible for a whole new range of activities and operations.*

Keywords: *Internet of Things, Blockchain, Security, Cyber-security*

I. Introduction

A blockchain is a cryptographically linked list of records that maintains an exhaustively empirical census without the need for a central authority. Because of its improvements over traditional designs, academics have been encouraged to adapt it to domains that emphasize security. The decentralized architecture, critical secrecy, rigidity, trust, security, autonomy, integrity, and scalability of this novel architecture are its key benefits. Smart Contracts for relationships between the Blockchain and third parties are supported by several legal cases.

A notable use case for Blockchain technology is the Internet of Things (IoT), which has grown quickly in recent years despite the security measures often being minimal owing to budget constraints. There are several reasons why IoT networks are exposed to external attacks, some of which are outlined in [1]. They usually use different wireless communication protocols to connect to a gateway, which makes eavesdropping fairly simple, and they typically have little computing power, making it

challenging to deploy extensive security measures on an individual device basis. Furthermore, while personal prejudices are typically protected, it is straightforward to physically access them.

The basic security advantages of using a Blockchain architecture in IoT ecosystems, and particularly in smart home installations, are covered in this essay. Additional use cases to improve IoT installation security are described, and the key advantages of incorporating a blockchain into such systems are examined.

II. RELATED WORK

In contrast to IoT networks, which have highly centralized architectures for regulating device data, the new Blockchain distributed ledger technology provides major built-in security advantages. [2] conducts research on the use of blockchain technology in the IoT space to encourage resource sharing and automate a variety of arduous tasks in a secure manner. The blockchain-IoT combo is powerful, the authors' findings show, and it may pave the way for fresh business ideas and distributed applications. Additionally, [3] reviewed pertinent studies and works produced for Blockchain applications in IoT. Numerous research studies [4-6] using Blockchain architecture to manage data storage were included in the paper. In order to ensure the security and integrity of their connection, data exchanged between IoT devices is always recorded as unique transactions inside the Blockchain and subsequently distributed among the nodes.

Nearly all relevant research works leverage blockchain technology as a data storage management solution by utilizing the underlying architecture that enables decentralization, resilience, trust, security, scalability, autonomy, and integrity. This study offers additional use cases for enhancing IoT smart home security, particularly in respect to how they interact with caregivers and other external parties.

III. IOT ENVIRONMENT SECURITY

An IoT installation is made up of networked, unrelated devices that communicate with the gateway, network peers, or other connected devices to exchange private user information. There are several configurations and deployment techniques available for contemporary IoT systems. Decentralized deployment, high connection, variety, and diversity raise several security and sequestration issues. Flexibility, sequestration, identity management, network security, and trust are the five categories into which they may be separated. The conditions for resolvable network security are confidentiality, integrity, authenticity, and vacuity. The many identity operation scenarios include authentication, authorisation, responsibility, and cancellation. The sequestration prerequisites are satisfied, including data sequestration, anonymity, pseudonymity, and

unlikability. Device, reality, and data trust are the three types of prerequisites for trust. The prerequisites for adaptability are ultimately resolved by robustness against assaults and adaptability against failures [7].

Blockchain component for IoT

A Blockchain element and a risk assessment tool may be included into the core of IoT installations to offer a brand-new degree of security. By decentralizing and mirroring reliable viewpoints on the Blockchain network, it can protect the integrity of such a medium. Additionally, the Blockchain component may be used to record data overflow that occurs between IoT bias and the IoT gateway. Depending on the specified filtering criteria, the collected data flows can reflect some or all of the modified dispatches; these can then be preserved as deals and broadcast to the Blockchain distributed tally.

Possible Blockchain boost commerce in smart houses is depicted in Fig. 1. How each smart home's IoT bias communicates with an IoT gateway and modifies data overflow is depicted in the Figure. The gateway may act as both a gateway and a Blockchain bump if it has enough processing power or doubles as a light Blockchain bump. In this alternative script, it's crucial to employ fresh, complete Blockchain bumps that may be disseminated or centralized across the bases of all smart houses. To broadcast these transactions and employ these bumps as miners to reach consensus in transaction confirmation situations, the distributed Blockchain ecosystem of smart homes may be leveraged.

IV. Using blockchain to improve security and privacy in smart homes

The many methods an IoT device network may leverage Blockchain technology to address the security and segregation requirements of a smart home environment are described in this Section.

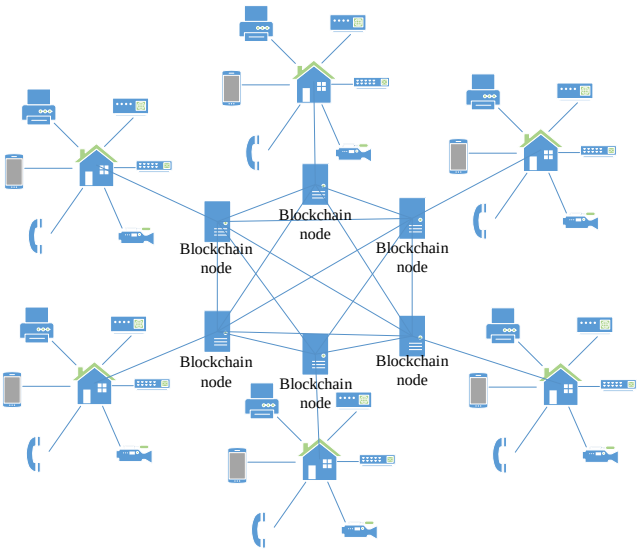

Fig. 1. Blockchain nodes interaction

Resilience

There are a number of commonly used techniques that can aid with some of the flexibility needs of IoT systems, including intrusion discovery, monitoring, and the discussion of system events. This enables and facilitates efforts to connect [8] and circumvent system security without authorisation. The two primary approaches to intrusion discovery algorithms are anomaly discovery grounded (where network activity is continuously monitored and compared against an established baseline of normal business profile) and signature discovery grounded (where a repository of signatures describing particular security pitfalls is maintained) [9]. However, both solutions need a lot of resources, making it hard to use them with IoT bias's extremely low computing power.

High-processing Blockchain bumps might act as the IoT network's foundation. In addition to correlating and recording deals in line with the accepted Blockchain protocol, these bumps are also utilizing their processing power to run intrusion-detection algorithms. The public tally syncs across all gateway bumps and holds a list of all transactions in the network in chronological order, allowing the intrusion detection algorithms to run concurrently and expediting their procedure.

The system's overall energy consumption is directly impacted by the deployment of Blockchain surges with high processing power to increase IoT installation flexibility. However, the energy surge may be controlled if a mining method with a lower difficulty is adopted, and just a few Blockchain spikes are used. Both of these safeguards are applicable for a private Blockchain network where access to unauthorized drug users is forbidden.

Identity Control

Device authentication is a method for meeting the IoT environment's identity operation need. To prevent the installation of illegal or unsecured bias, the Internet of Things (IoT) network must be connected to a reliable bias source. Due to the decentralized nature of IoT installations and the absence of robust authentication procedures in IoT gateways, its enforcement is difficult. The original whitelist created by the Knowledge Base contains a selection of IP addresses that have been deemed safe. The threat of machine-verified bias on the network and the direct end-stoner installations through the Control and Examiner sub-caste cause this list to grow over time.

The blacklist itself is made up of IP addresses that the threat machine identified as potentially harmful after comparing network activities on a device with user profiles that may be accessed through a Contextual Profiling subclass. In order to update the

blacklist based on the most recent intelligence, the Threat Machine and the Knowledge Base can also interact.

The whitelist and blacklist are both retrieved from the threat machine via the pertinent calls for each Smart Contract that needs them. A static list of IP addresses with a limited lifespan is hard-enciphered in a smart contract in the event that the lists aren't accessible. After such a Contract expires, a new bone is placed with a condensed list to stop any more bumps that were marked as potentially harmful. a similar infrastructure built on Blockchain and Smart Contracts for a collaborative DDoS mitigation method that employs IP address blocking to halt suspicious traffic, as detailed in [10].

Network Security

IoT bias's firmware has a major role on how it functions. A device's firmware can be upgraded after it is put to use to fix bugs, improve stability, or add new features. But at the same time, if a cunning stoner [11] successfully hijacks the upgrade procedure, the network's security may be at risk. A skilled bushwhacker can disable the streamlining firmware and replace it with a risky interpretation that makes the device operate in an unpredictable manner because many of these biases are always-on, have limited processing power, and the device manufacturers are reluctant to increase their security due to cost considerations.

IoT bias firmware attacks have been well studied. [12] illustrates how the firmware verification procedure may be evaded since the tackling structure of the Nest thermostat offers no resistance. According to a security study of IoT biases done in [13], attacks can target both consumer and artificial IoT biases. Furthermore, [14] showed that it is simple to prevent Philips Hue lights from updating their firmware by connecting infected bulbs to the network, using the universal AES-CCM key that Philips uses to encrypt and authenticate new firmware to carry out a side-channel attack, and taking advantage of flaws in the Touchline section of the ZigBee Light Link protocol.

IoT networks can employ a revolutionary firmware updating method built on the Blockchain network. By doing this, it will be feasible to securely evaluate the firmware's correctness and interpretation and make sure that all of the network's nodes have the most recent firmware installed.

Trust

Each IoT device could be given a unique identification ID number. The "Entity ID" of the device and the "Stoner ID" of the smart home stoner are used in a smart

contract to create the ID. For WiFi or Zigbee-capable devices, the "Entity ID" is the MAC address; for Bluetooth-capable devices, it is the Bluetooth Device Address; and for Z-Wave devices, it is the Network ID/Node ID brace. The "Entity ID" is defined by the underlying protocol of each device. This technique is open to the general public as a Smart Contract on the Blockchain network, and it is centrally administered by an authorized stoner similar to a network director.

The benefit of understanding a device's structure's exact condition overcomes the fact that registering it adds a new complexity subcaste to the IoT armature. Furthermore, biases may be managed both individually and collectively since they are interconnected. Eventually, by restricting connectivity to authorized bias, the network may be managed more easily and securely.

From the bottom up, blockchain networks are built on a flimsy evidence base of all recorded transactions, including any data that has been corrupted by human prejudice [15]. Smart contracts may be utilized in this kind of network to carry out any communication across biases and record those records as records in a public tally. In order to demonstrate that these recordings originated from each matching device and to prevent other implied threats like deputy or man-in-the-middle attacks and renewal attacks, the network cryptographically signs these recordings and authenticates the signatures [16].

There is often little motivation for lone drug users to improve security after release by simplifying device firmware or swapping out risky and susceptible bias with safer druthers on a previously released IoT system. A virtual currency may thus be used as a consequence. By assigning varying charges to specific biases based on threat assessments from prior tasks or on vulnerabilities that are known to exist, the use of a virtual currency aims to strengthen network security. Drug users also have to pay a large virtual cost to compensate for the diminished secure bias. Virtual currency may be used on a network in a manner similar to how actual currency can be used on a device [17].

It is critical to inform the participating users of the network's operating tenets and request their agreement in order for an IoT device network to operate. Digital signatures can be used to complete a Form of Consent. The signature is completed whenever the rules are altered and whenever a user joins to the network for the first time. Only once users have signed the most current Form of Consent are their IoT devices allowed to use the network [18–20].

The following method is used to digitally sign the Form of Consent:

•After receiving the request for an external connection, the blockchain service asks the user to electronically subscribe to or accept a Form of concurrence via a Smart Contract.

•Once the stoner signs the paperwork, the transaction is officially registered.

•The remaining decentralized bumps will ultimately infiltrate the block that is hosting the sale and booby-trap it.

Privacy

Smart home IoT devices routinely store sensitive personal data about their users. A system for managing permits must be devised as a result. As a result, before any IoT device in the user's smart home may share data with third parties, the user must approve permission. Using a smart contract, this access may be granted or revoked with the following inputs:

•Device ID. There is a unique identification number for the bias in a drug user's smart home network.

•A third party's ID. This unique code serves as a portal to a new universe.

•State. This field, which might take on the values "entitlement" or "drop," indicates the status of data access.

•A deadline. It is possible to indicate the time window during which the access status will change using this optional input. However, if the input is ignored, the status change is irreversible and can only be reversed by making a new call to the smart contract.

TABLE I. Internet of Things Security Classification

IoT Security Issues	
Issues With Low Level Security	Jamming adversaries
	Insecure initialization
	Low-level Sybil and spoofing attacks
	Insecure physical interface
	Sleep deprivation attack
Issues with Intermediate Security	Replay or duplication Attacks due to fragmentation
	Insecure neighbor discovery
	Buffer reservation attack
	RPL routing attacks
	Sybil attacks on Intermediate layers
	Authentication and secure communication
	Transport level end-to-end security
	Session establishment and resumption
	Privacy violation on cloud-based IoT
Issues with High-Level Security	CoAP security with internet
	Insecure interfaces
	Insecure Software
	Middleware Security

V. CONCLUSION

In order to improve the security of IoT in smart home installations, this paper presented a decentralized platform based on Blockchain and Smart Contracts.

Because comparable systems have distinct structural and functional properties, IoT installations in smart homes come with a range of security and sequestration requirements that are difficult to achieve. By helping to fulfill some of these objectives, blockchain technology may be utilized in comparable circumstances to boost security and efficiency. Alternative plans have been proposed and mentioned.

REFERENCES

[1] Atzori, L., Iera, A., Morabito, G.: The Internet of Things: a survey. Comput. Netw. 54(15), 2787–2805 (2010)
[2] Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things. IEEE Access 4, 2292-2303 (2016)
[3] Conoscenti, M., Vetr6, A., Martin, J.C.D.: Blockchain for the Internet of Things: a systematic literature review. ln: 2016 IEEE/ ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1-6, November 2016
[4] Worner, D., von Bomhard, T.: When your sensor earns money: exchanging data for cash with Bitcoin. In: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ublquitous Computing: Adjunct PuЬlication, UЬiComp 2014 Adjunct, pp. 295-298. ACM, New York (2014)
[5] Zhang, У., Wen, J.: The IoT electric business model: using ЬIockchain technology for the Internet of Things. Peer-to-Peer Netw. Appl. 10(4), 983-994 (2017)
[6] Zyskind, G., Nathan, O., Pentland, A.: Enigma: decentralized computation plat-form with guaranteed privacy. arXiv preprint arXiv:1506.03471 (2015)
[7] Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., Kikiras, P.: On the security and privacy of Internet of Things architectures and systems. In: 2015 International Workshop on Secure Internet of Things, pp. 49–57 (2015)
[8] William, S.: Computer Security: Principles and Practice. Pearson Education India, Delhi (2008)
[9] Kumar, S.: Survey of current network intrusion detection techniques. Washington University in St. Louis (2007)
[10] Rodrigues, B., et al.: A blockchain-based architecture for collaborative DDoS mit-igation with smart contracts. In: Tuncer, D., Koch, R., Badonnel, R., Stiller,

B.(eds.) AIMS 2017. LNCS, vol. 10356, pp. 16–29. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-60774-0 2

[11] Lee, B., Lee, J.H.: Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. J. Supercomput. 73(3), 1152–1167 (2017)

[12] Hernandez, G., Arias, O., Buentello, D., Jin, Y.: Smart nest thermostat: a smart spy in your home. Black Hat USA (2014)

[13] Wurm, J., Hoang, K., Arias, O., Sadeghi, A.R., Jin, Y.: Security analysis on consumer and industrial IoT devices. In: Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific, pp. 519–524. IEEE (2016)

[14] Ronen, E., Shamir, A., Weingarten, A.O., O'Flynn, C.: IoT goes nuclear: creating a ZigBee chain reaction. In: 2017 IEEE Symposium on Security and Privacy (SP), pp. 195–212. IEEE (2017)

[15] Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., Sebastopol (2015)

[16] Kshetri, N.: Can blockchain strengthen the Internet of Things? IT Prof. 19(4), 68–72 (2017)

[17] Nurshod Akhmedov, Halim Khujamatov, Amir Lazarev, Madiyar Seidullayev. Application of LPWAN technologies for the implementation of IoT projects in the Republic of Uzbekistan // 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan –2021.

[18] Bakhodir, Y., N. Nurbek, and Z. Odiljon. "Methods for applying of scheme of packet filtering rules." International Journal of Innovative Technology and Exploring Engineering 8.11 (2019): 1014-1019.

[19] Yakubdjanovna, Irgasheva Durdona, Nasrullayev Nurbek Bakhtiyarovich, and Xolimtayeva lqbol Ubaydullayevna. "Implementation of intercorporate correlation of information security messages and audits." 2020 International Conference on Information Science and Communications Technologies (ICISCT). IEEE, 2020.

[20] Baxtiyorovich, Nasrullaev Nurbek, and Holimtaeva Ikbol Ubaydullaevna. "Method of analyzing of antivirus errors when audit provides." 2019 International Conference on Information Science and Communications Technologies (ICISCT). IEEE, 2019.