

A Survey on Blockchain for Solving Safety Problem of iot

Vaibhav Jagtap¹, Shreya B. Ahire²

1. Department of Computer Engineering, NBNSOE, Ambegaon, Pune, Maharashtra, India

2. Department of Computer Engineering, NBNSOE, Ambegaon, Pune, Maharashtra, India

Abstract

Today, blockchain technology attracts a lot of attention from investigators, computer experts, and local professionals in a variety of businesses, including lending, business, real estate, transportation, supply chain, and healthcare. This curiosity is because bitcoin and its equivalent platform were the first applications of blockchain and the framework of cryptocurrencies. In contrast to the critical structure used in the maximum system, the distributed structure and the cryptographic hash algorithm used are particularly preferred in the security field. Use an experimental approach to create a chain of trust to protect iot devices, iot device transaction validation, and iot device mesh network protection via blockchain technology. Forensic examination uses immutable transactions to determine its effectiveness. The biot concept has four advantages: publishing and replicating sensor data for public and distributed ledgers, timestamps using blockchain structure, data verification, and non-denial.

Keywords: Internet of Things, Security, Blockchain, Healthcare

I N T R O D U C T I O N

Blockchain and Internet of Things (iot) are powerful, and the combination of these technologies can be used in incredible ways by companies. It may be called a blockchain or BIOT of things. By definition, iot is a network of connected things. Assembled by CPU, memory (RAM, ROM, EEPROM, flash) and IO bus. The aforementioned consists of a minimum of single network interface, including Wi-Fi, Bluetooth and zigbee, and is armed through sensors and actuators. On the way to achieve a secure and reliable iot framework, objects must support three elementary functions:

1. Secure communication for information exchange, i.e. Robust mutual authentication amongst end entities, confidentiality, and integrity.
2. Required for secret values that are enforced through tamper-resistant devices, for instance secure storage and secure elements used for communication.
3. Physical technologies that deal with logic technologies such as multiprocessors and sandboxes can effectively contribute to increased intrusion resistance.

Since its use in cryptocurrencies, blockchain has gained great appeal due to the prospect of versatile applications. As the Internet of Things (iot) emerges for variety of requirements and devices, data security is likely to be a major concern. The shape and block structure of the blockchain are as follows:

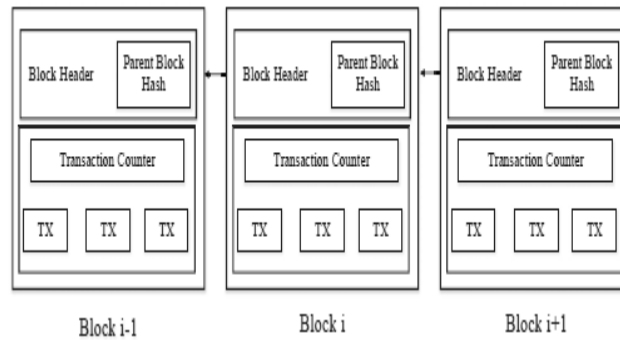


Fig 1 Blockchain

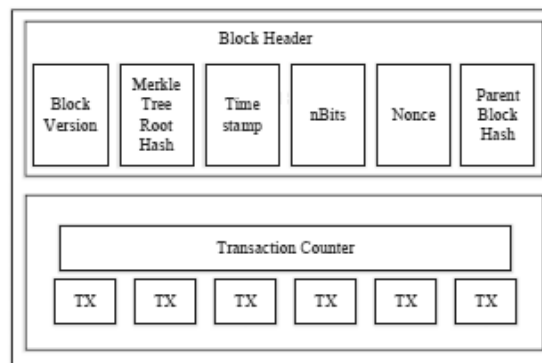


Fig 2 Blockchain Structure

II MOTIVATION

As a performance that applies the system in real-world scenarios where information is jointly provided between individual components in the system. The surveyed paper has designed a system that integrates current data sharing systems and uses Ethereum virtual machines to provide safe and efficient services. To protect the system's data, the system transfers from one user to another for blockchain and smart bonding. Blockchain and the Internet of Things are the furthestmost important and most attracted technology in the world today. Learning trend technology is very important.

III L I T E R A T U R E S U R V E Y

Below Table 1 shows the various papers survey based on the method

IV SYSTEM ARCHITECTURE

The architecture explained the concept of four quarter architecture and established the idea of smart thermometers. Rendering to this model, the entity is to build into four physical and logical layers.

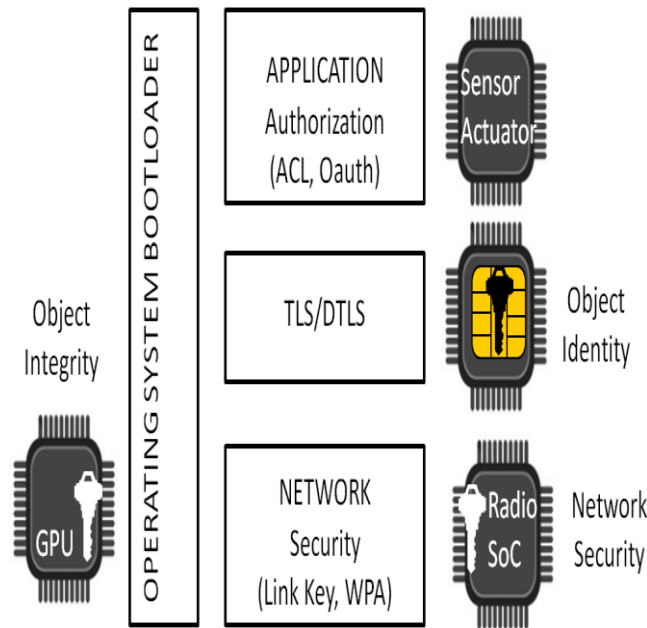


Fig 3 BC Based four quarter Architecture for IoT

A generic unit (GPU) that manages objects on a core processor that turns the required small operating system or software. As shown, atmega2560 chip delivers 256KB of flash and 8KB SRAM. The latest actions might be secured (required) in encryption (and must be required).

Wireless soc (e.g., 36 KB of SRAM related with peripheral 4 MB SPI flash) including processors through RAM and exterior non-volatile memory. This is usually responsible for MAC security that handles asymmetric encryption. Supports software update procedures.

The identity module, i.e. Secure elements (Java cards running TLS stacks), these tamper-resistant components surround the number of flash memory and 10 KB SRAM. The TLS stack rendered to Java card language in addition to applying an application firewall between the wireless soc and GPU.

- Sensors and actuators are determined by core processor rendering to REST communications forwarded through wireless packets. As mentioned earlier, authorization mechanisms are optionally reinforced.

The four-quarter architecture protects each other from GPU and wireless soc air software updates. You can't evade malicious updates made by hackers who have animal access to your device[10 11]. This feature infers the accessibility of classic, secure download operations on stored symmetric private keys. And rummage-sale in electronic chips.

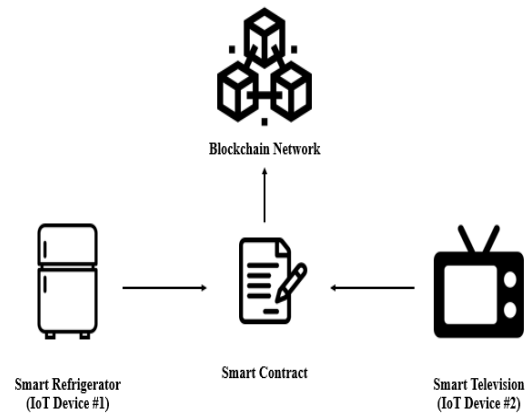


Fig 4 iot system using blockchain technology

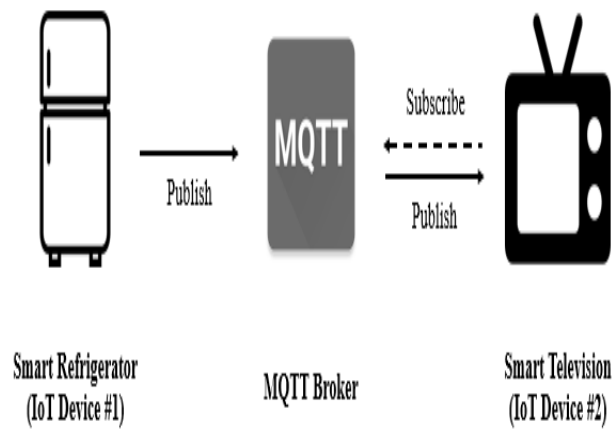


Fig 5 iot system without blockchain technology

Sr. No	Year	Author	Paper	Methods	Vol. 13, No. 3s, (2020), pp. 1663–1669	
					Advantages	Disadvantages
1	2018	Pascal Urien	Blockchain iot (biot): A New Direction for Solving Internet of Things Security and Trust Issues.	Draw bridge concept by using TLS/TLDS	To analyse CIA Security Triad (Confidentiality, Integrity, Availability) Of our architecture to show resilience against some attacks.	The paper uses private BC in hospitals and health centres Miners are not from outside the organization to create malicious blocks.
2	2017	Nir Kshetri	Can Blockchain Strengthen the Internet of Things?	Supply chain technology	Reducing risk with superior security.	Double spending, cracking of the cryptographic etc.
3	2017	P. Urien	Securing The iot With TLS/DTLS Server Stacks Embedded In Secure Elements: An eplug Usecase.	An eplug Usecase using TLS/DTLS technology.	Identity management, resilience.	Blockchains use excessive energy.
4	2013	K. Pretz	The Next Evolution of the Internet.	Distributed Ledger technology.	Transparency, autonomy.	Blockchain is not a huge distributed computing system.
5	2016	C. O'Flynn	A Lightbulb Worm? Details of the Philips Hue Smart Lighting Design.	Supply chain technology	Reduce risk of collusion and tampering.	It is not indestructible.
6	2017	E. Ronen	Iot Goes Nuclear: Creating a zigbee Chain Reaction	An eplug Usecase using TLS/DTLS technology.	Streamlines accounting.	Blockchain entries are not immutable.
7	2018	8. N. M. Kumar and P. K. Mallick	Blockchain technology for security issues and challenges in iot.	Drawbridge concept by using TLS/TLDS	A more efficient supply chain.	Scalability remains blockchain's weakness.

Table 1 Literature Survey

V CONCLUSION

The growth of the Internet of Things is accelerating, but there are security issues. One of the security issues that occur is that the communiqué between iot devices becomes unstable. In this study,

we design and implement iot systems without using blockchain technology and without comparing the results. Shorn of iot systems in blockchain technology that uses MQTT as a communication protocol. On the other hand, iot systems equipped with blockchain technology use Ethereum as a platform for blockchain networks. In addition, smart contracts are used to store and retrieve the necessary information from a blockchain network. Based on the various tests performed, you can:

Iot systems that use blockchain technology provide a higher level of security than iot systems that do not have blockchain technology that can guarantee data integrity. This white paper demonstrates that we can resolve security issues caused by communication between iot devices. This can be understood from attack simulation and observation tests that use blockchain technology to recover the security of iot systems.

VI FUTURE SCOPE

The growth of the Internet of Things is accelerating, but there are security issues. One of the security issues that occur is that the communiqué between iot devices becomes unstable. In this study, we design and implement iot systems without using blockchain technology and without comparing the results. Shorn of iot systems in blockchain technology that uses MQTT as a communication protocol. On the other hand, iot systems equipped with blockchain technology use Ethereum as a platform for blockchain networks. In addition, smart contracts are used to store and retrieve the necessary information from a blockchain network. Based on the various tests performed, you can:

Iot systems that use blockchain technology provide a higher level of security than iot systems that do not have blockchain technology that can guarantee data integrity. This white paper demonstrates that we can resolve security issues caused by communication between iot devices. This can be understood from attack simulation and observation tests that use blockchain technology to recover the security of iot systems.

REFERENCES

- [1] P.Urien, "An Innovative Security Architecture for Low Cost Low Power iot Devices Based on Secure Elements", demonstration at the IEEE CCNC 2018 conference and at the CES2018 comsoc Kiosk.
- [2] Nir Kshetri, "Can Blockchain Strengthen the Internet of Things", IEEE IT Pro, July/August 2017.
- [3] P. Urien, "Securing The iot With TLS/DTLS Server Stacks Embedded In Secure Elements: An eplug Usecase", IEEE CCNC 2017.
- [4] K. Pretz, "The Next Evolution of the Internet", the institute.ieee.org 2013.
- [5] C. O'Flynn, "A Lightbulb Worm? Details of the Philips Hue Smart Lighting Design", Black Hat USA 2016.
- [6] E. Ronen, C. O'Flynn, A. Shamir, A. Weingarten, "iot Goes Nuclear: Creating a zigbee Chain Reaction", 2017 IEEE Symposium on Security and Privacy.
- [7] IETF draft, "TLS and DTLS Security Modules", draft-urien-uta-tls-dtlssecurity-module-04.txt, June 2017.
- [8] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in iot," Procedia Computer Science, vol. 132, pp. 1815 – 1823, 2018, international Conference on Computational Intelligence and Data Science.
- [9] Yong Yu, Yannan Li, Junfeng Tian and Jianwei Liu. Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things. IEEE Wireless Communications, Year: 2018, Volume: 25, Issue: 6, Pages: 12 – 18, IEEE Journals & Magazines.
- [10] Dhumane, A., & Prasad, R. (2015). Routing challenges in internet of things. CSI Communications.

- [11] Dhumane, A. V., Prasad, R. S., & Prasad, J. R. (2017). An optimal routing algorithm for internet of things enabling technologies. *International Journal of Rough Sets and Data Analysis*, 4(3), 1–16.