

Survey of Solutions to IoT Security Issues using Blockchain

Pinkal Chauhan

Dept. of Computer Engineering, LDRP-ITR Sector 15, Gandhinagar, Gujarat, India

Abstract

Internet of Things (IoT) is indicating exponential development in industry and research fields, yet regardless it experiences security vulnerabilities. IoT gadgets procedure and trade information without human cooperation. Security issues will keep on expanding with such a template, particularly for confidential information, such as information gathered with increasingly more refined associated gadgets (framing the IoT). In this way IoT elements need to perceive and validate an authenticate and trade of information. Blockchain based decentralized framework ready to meet security safeguarding in IoT environment. The distributed system suggested uses Ethereum to overcome conventional networks by a Blockchain variant of smart contracts.

Keywords

Blockchain, IoT (Internet of things), IoT, Security, Privacy.

I. Introduction

IoT (Internet of Things) is a lightweight system comprising of

sensor gadgets that can be associated with the Internet and can convey wirelessly. IoT system made out of lightweight gadgets is a structure that totals and manage information produced by sensor gadgets on a central node which act as a core admin. IoT gadgets are gadgets that have constrained assets, for example, constrained battery limit, low processing power, and less space to store data and experience issues in applying high-performance programming. Since high-performance security calculations can't be utilized with restricted assets, there is an issue that security is low in lightweight systems, for example, IoT. The Blockchain created as Bitcoin's key technology has excellent security and is showing tremendous interest in regions requiring high-efficiency quality in safety. High Blockchain protection is seen as an appropriate method for applying it to systems that are low in security such as an IoT.

Blockchain guarantees strong security capacities by utilizing anticorruption, integrity, distributed storage, and time based monitoring of secure device development transactions [1].

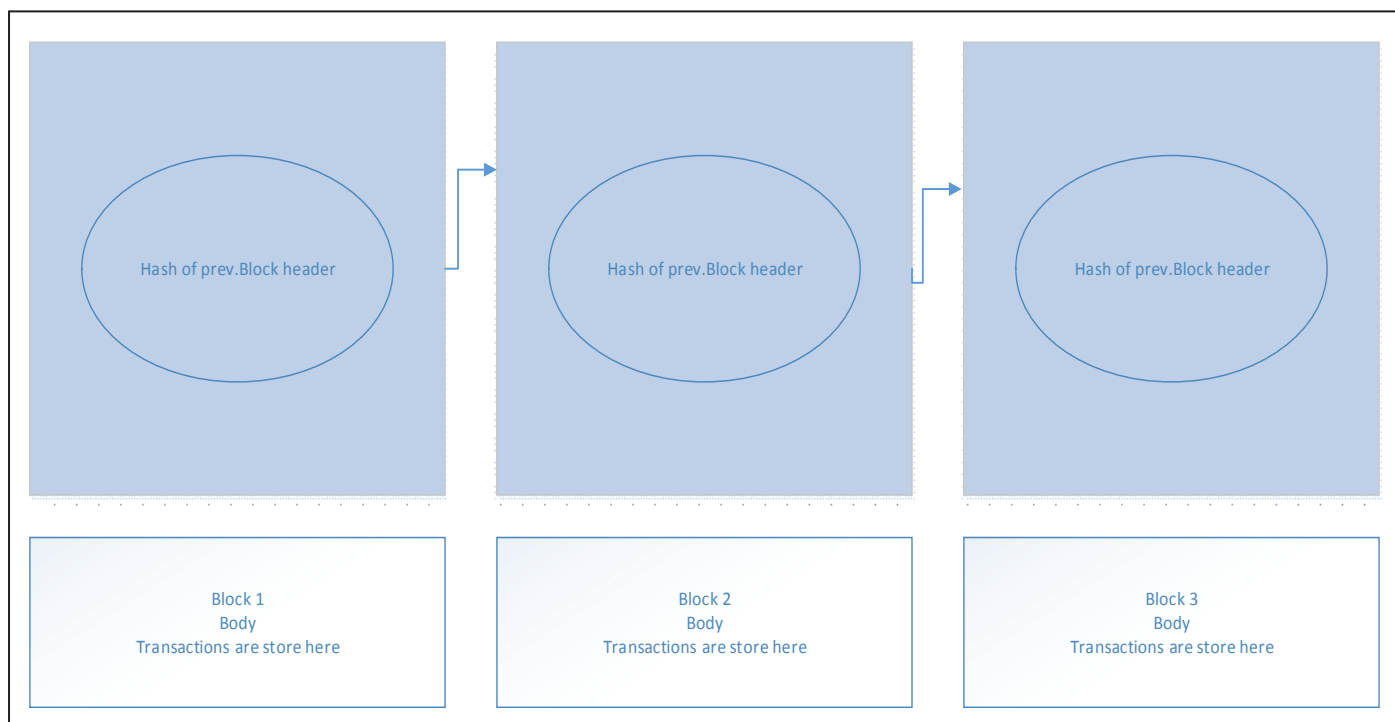


Fig. 1: Transaction Diagram of Blockchain

A. Blockchain

A decentralized repository which maintains a permanent and manipulative transaction data record is called as Blockchain. A Blockchain is completely distributed through the use of peer-to-peer system. Most specifically, each network node keeps a digital version of the booklet to prevent a single failure point. All version shall immediately reviewed. By theory, the Blockchain is a distributed data system and is referred to as a “distributed ledger” for the utility of network transactions [16]. CurrentBlockchain operation has been developed to address the double expense of cryptocurrency spending. Nevertheless, various works currently explore and use

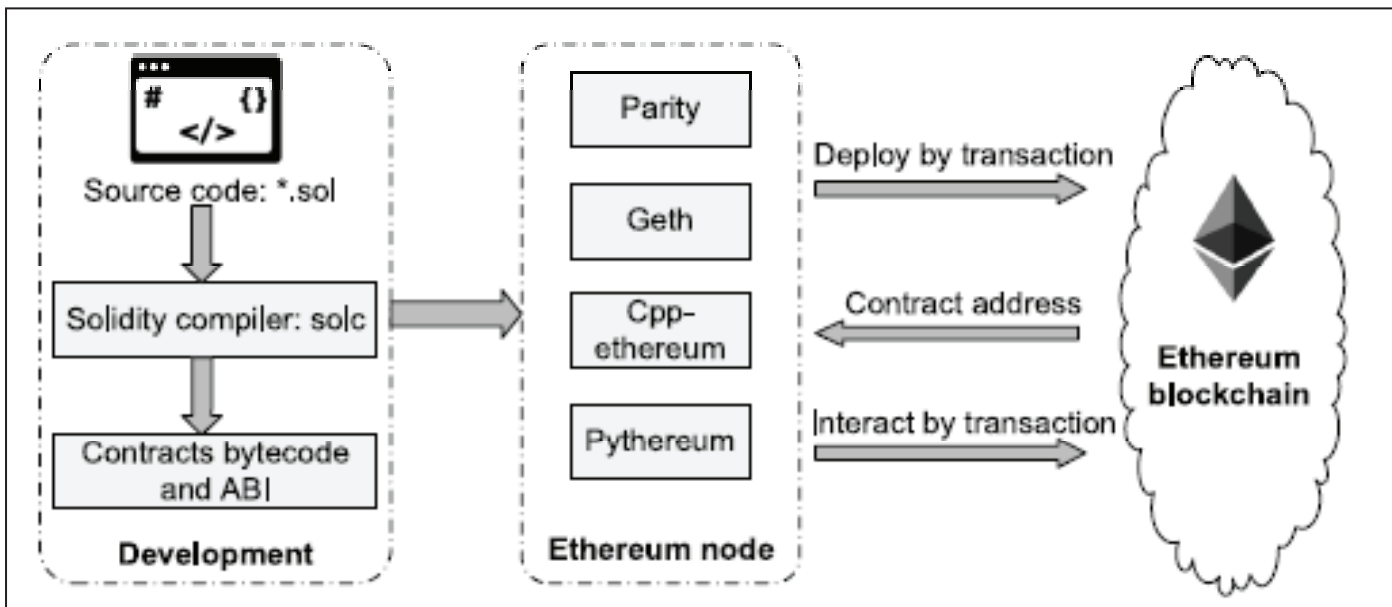


Fig. 2: Process of Smart Contracts' Development, Deployment and Integration

Blockchain technologies as a safe way to create, manage and maintain a decentralized repository of every kind of digital transactions [3]. There are various methods to prove the truthful validity of frames. The Proof of Work (PoW) and the Proof of Stake (PoS) methods most often used.

A miner, any peer in a peer-to-peer system, will have to answer for a computer-intensive cryptographic puzzle called a Proof of Work (POW) for the mining of BC blocks. Newly developed blocks are distributed to all network nodes. After all the miners have tested the block, the BC is inserted. When a block has been inserted in the BC, it is quite difficult to change block data because all subsequent blocks need to be changed. And any block linked to a BC needs the approval of the network's majority nodes.

A Blockchain consists of blocks that contain details of network transactions. Token Transfers in a network or any type of data exchange may be the transaction information. Logically, each block consists of a header and a body, two parts. Transactions shall be stored in the block body, and the header of the block shall contain the previous block identifier, along with other properties. The frames, as shown in fig. [1], are therefore linked in a chain like a linked list.. The first block is known as the "genesis" block [17] in the chain.

Blockchain may be allowed (private) or less (public). In the first classification, consensus contributors are excluded. The rights to verify transactions only lie in the designated confidential actors. It takes little effort to reach a consensus, so neither energy consumption nor time is needed. Finally, it allows for the confidentiality of transactions, as only licensed parties can access the transactions. The second type of the system uses an unlimited number of anonymous nodes (public Blockchains). Every actor can communicate safely on the basis of the cryptography. A pair of private/public keys is shown for each node. Each actor in the Blockchain can read, write and verify transactions. The Blockchain is secure and the consensus in the network is achieved, though 51% of the nodes are truthful. Normally unauthorized Blockchain consume energy and time, because they include a calculation to improve system security.

B. Smart Contracts

On the Blockchain itself, smart contracts are keys enforced, which enable the computation of general uses. It may have conditions or consequences based on acts, similar to a contract between any two people. Nevertheless, in Blockchain smart contracts are entirely put online. Smart contracts are critical in managing data-based interactions between nodes and system participants. Like any other node, smart contracts have Blockchain addresses. Transaction is used to initiate smart contract [6]. It uses binary interfaces (ABIs) that are provided by smart contract for communication. A record transaction or other contract message may be executed to submit such ABIs. We can be executed without sending transactions and messages by simply invoking the call feature [7].

The fig. 2 explain the working of smart contract's development, deployment and interaction. Every contract which is deployed, corresponds to a unique address, from that user can communicate with contract through transactions by different client(e.g. Parity, Geth, etc.) Compared with the traditional apps, Apps has certain characteristics and advantages like Autonomy, Stable, Secure, Traceable System [8].

C. Ethereum

Ethereum is a decentralized Blockchain offering the digital currency called Ether (ETH), which is used for the payment of financial transaction and software storage (after the fork that took place in July 2017), Ethereum is popular as Ethereum classic. Miners copy, verify and store information in the network Blockchain. In addition, programs called smart contracts are processed, making Ethereum a platform for distributed applications. Smart contracts are carried out by participating nodes using the Ethereum Virtual Machine (EVM) operating system [3]. Apps running as updated without the risk of down time, constraints, coercion or outer interference are a distributed system that runs smart contracts. Ethereum classic the classical edition Ethereum maintaining untemper past follows the original Ethereum Blockchain; external interference free and activity subjective interference free. Ethereum can also be used as a personal ledger, thus choosing the participating nodes and no longer requiring pow algorithm [4].

D. IoT Blockchain

Blockchain has recently attracted in significantly more consideration in various parts because of its productivity in a decentralized framework without including a third party. A case study to apply Blockchain to IoT was proposed to overcome the weakness of the IoT framework. The primary vulnerability you need to overcome for is security issue because of the low execution of lightweight gadgets. It can solve issues of the current centralized structure by applying distributed attributes of Blockchain to IoT system and relieve constrained battery issues of existing IoT gadgets that require constant correspondence with central nodes by removing it. Thus, different research is being done to apply Blockchain to IoT. For upgrading security, many research are being done to create lightweight Blockchain for IoT and to grow the scope of IoT framework use. There are study on the improvement of security of IoT network that attempts to apply decentralized attributes of Blockchain to IoT so as to take care of issues of centralization [1]. It uses other mechanisms such as Proof of Work and proof of stake to display block's authentication [3].

Blockchain based solutions in Internet of things, like privacy, security, management of data, trustless platform and monetization in IoT [5].

II. Related Work

The author of paper [3] proposed unique way called bubbles of trust, the place where gadgets can interact fully securely in protected digital areas. Such a method can be used to various IoT context, administrations and situations. It depends on public Blockchain, subsequently, it profits by the entirety of its security properties. C++ with ethereum framework is used for performing it. The assessment of their methodology demonstrates its capacity in gathering the security prerequisites just as its flexibility toward attacks. Also guarantees an identification and verification of gadgets.

The author of [6] target to think about how conceivable it is to utilize Blockchain innovation in the area of security in IoT. They have displayed an architecture arrangement intended for that depends on contract model between a communication nodes. To adapt the large size of information to store, they have proposed to relate the Blockchain with corresponding storage. They have proposed data sharing mechanism based on idea of Embark framework. In these system block contains primary contract information just as reference to where the total information to insert. They also introduced a logical model to study performance that has a highly affects the general reaction time of the foundation [6].

The author of [13] proposed IoTChain, a combo of OSCAR architecture [11] and ACE authorization framework [12]. To provide a way to connect IoT gadgets safely. IoTChain comprises of two parts, an authorization Blockchain dependent on the ACE system and the OSCAR object security model. They thought to make the ACE approval stage trustless and adaptable. To this reason, they utilize a Blockchain to single ACE approval. Smart contract approve requests are handle by Blockchain. Blockchain is developed on top of a private ethereum network. Proposed system provides a flexible way to authorized clients.

The author of [14] paper expects to address DDos security issues in IoT gadgets with Blockchain. They utilize ethereum, a Blockchain variation, with smart contract to replace conventional IoT infrastructure with Decentralized manner. The combination of IoT and smart contract prevents unauthorized access gain. The proposed framework can give qualification between trusted and

untrusted gadgets and assign some fixed limit of resources to every gadget. It provides strong base to prevent and detect DDos attacks on Iot gadgets.

The author of [15] examines Internet of Things (IoT) access control issue. Specifically, they gives a brilliant agreement system. To accomplish trustworthy access control for Iot gadgets, it uses access control contracts (ACCs), judge contract (JC) and register contract (RC). In addition, a case study accommodated the autonomy with one workstation, one Computer and two single-board PCs via Raspberry Pi in an IoT structure. The case study explains the proposed system in accomplishing reliable access control for the IoT.

III. Our Proposal

IoT plays a very important role in our daily lives. it is important to sense and collect data from connected devices, and the share the data across the internet. All those entities must be recognize and authenticate each other as well as check integrity of data. There will be malicious users and malicious use. Most of the existing mechanisms propose a centralized client/server type approach where the server keeps a record of all the activities. Failure of such centralized server makes the system to fail. This kind of centralized authority is weak it means that any information in the network is vulnerable to hackers. Hence, it is required to have a decentralized/distributed approach where a single point of failure is avoided and public verifiability is offered. In Blockchain decentralized security option is there and it is impossible for hackers to target any individual on the network. we wish to offer an access control mechanism that is distributed in nature and provides public verifiability.

IV. Experimentation & Result

To demonstrate the application of the framework, we provide a case study in an IoT system with one desktop computer, one laptop, RFID reader and one single-board Raspberry Pi computers are implemented to achieve access control on the basis of the Ethereum smart contract platform. Data will be read and write using RFID reader from the RFID tag and it will be display on raspberry pi. Generated IoT data moving into the Blockchain. When data will be transferred we assumed attacks are occur and it break the security so generated data converted into encrypted form then after encoded data will be transferred into Blockchain network.

V. Conclusion

Blockchain is viewed as exceptionally adaptable technology which adaptable in numerous zones. One is that it is a crucial technology that can supplement vulnerabilities in low-level regions of protection. Here, We intend to proposed a system which should provide distinction between trusted and untrusted devices and allocates a static resource limit to each device which it cannot operate. We wish to propose a smart contract-based framework to implement distributed and trustworthy access control. The evaluation of our approach shows its ability in meeting the requested security requirements as well as its resiliency toward attacks.

References

- [1] Sunghyun Cho, Sejong Lee, "Survey on the Application of Blockchain to IoT", in 2019 International Conference on Electronics, Information, and Communication (ICEIC).

- [2] AymenBoudguiga, Nabil Bouzerna, Louis Granboulan, Alexis Olivereau, FlavienQuesnel, Anthony Roger, Renaud Sirdey, "Towards Better Availability and Accountability for IoT Updates by Means of a Blockchain", 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).
- [3] Hammi, Mohamed Tahar et al., "Bubbles of Trust: A decentralized Blockchain-based authentication system for IoT", *Computers & Security* 78, pp. 126-142, 2018.
- [4] EthereumClassic [Online] Available: <https://www.ethereumclassic.github.io/>
- [5] Ali, Muhammad Salek et al. "Applications of Blockchains in the Internet of Things: A Comprehensive Survey." *IEEE Communications Surveys & Tutorials* 21, pp. 1676-1717, 2019.
- [6] Rifi, Nabil et al., "Towards using Blockchain technology for IoT data access protection", 2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB), pp. 1-5, 2017.
- [7] Zhang, Yuanyu et al., "Smart Contract-Based Access Control for the Internet of Things", *IEEE Internet of Things Journal* 6, pp. 1594-1605, 2018.
- [8] Li, Xiaoqi et al. "A Survey on the Security of Blockchain Systems." *ArXiv abs/1802.06993* (2017): n. pag.
- [9] Dasgupta, Dipankar et al., "A survey of Blockchain from security perspective", *Journal of Banking and Financial Technology* 3, pp. 1-17, 2019.
- [10] Weaknesses. (n.d.). (2018), [Online] Available: <https://en.bitcoin.it/wiki/Weaknesses>
- [11] M. Vućinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, R. Guizzetti, "OSCAR: Object Security Architecture for the Internet of Things," *Ad Hoc Networks*, Vol. 32, pp. 3 – 16, 2015.
- [12] L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, and H. Tschofenig, "Authentication and Authorization for Constrained Environments (ACE)," *Internet Engineering Task Force, Internet-Draft draft-ietf-aceoauth-authz-07*, Aug. 2017, work in progress. [Online]. Available: <https://datatracker.ietf.org/doc/html/draft-ietf-ace-oauth-authz-07>
- [13] Alphand, Olivier et al. "IoTChain: A Blockchain security architecture for the Internet of Things." 2018 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-6, 2018.
- [14] Javaid, Uzair et al., "Mitigating IoT Device based DDoS Attacks using Blockchain." *CRYBLOCK@MobiSys* (2018).
- [15] Zhang, Yuanyu et al., "Smart Contract-Based Access Control for the Internet of Things", *IEEE Internet of Things Journal* 6, pp. 1594-1605, 2018.
- [16] F. Tschorsch, B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, Vol. 18, No. 3, pp. 2084–2123, thirdquarter 2016.
- [17] T. M. Fernández-Caramés, P. Fraga-Lamas, "A review on the use of Blockchain for the internet of things," *IEEE Access*, Vol. 6, pp. 32 979–33 001, 2018.



Pinkal Chauhan, received her bachelor degree in Information Technology from Shankersinh Vaghela Bapu Institute of Technology, India, in 2018, the Master degree in Computer Engineering from, LDRP Institute of Technology & Research, India, in 2020, Her research interests include internet of things (IoT), Blockchain, Privacy and Security. At present, she is engaged in LDRP Institute of Technology & Research for Complete her master degree.